

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Kazumasa OMOTE

Application No.: To be Assigned

Group Art Unit: To be Assigned

Filed: December 9, 2003

Examiner:

For: SECURITY MANAGEMENT APPRATUS, SECURITY MANAGEMENT SYSTEM,
SECURITY MANAGEMENT METHOD, AND SECURITY MANAGEMENT PROGRAM

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN
APPLICATION IN ACCORDANCE
WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith
a certified copy of the following foreign application:

Japanese Patent Application No(s). 2003-046251


Filed: February 24, 2003

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing
date(s) as evidenced by the certified papers attached hereto, in accordance with the
requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: Dec. 9, 2003

By: 
Gene M. Garner, II
Registration No. 34,172

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 2 月 2 4 日
Date of Application:

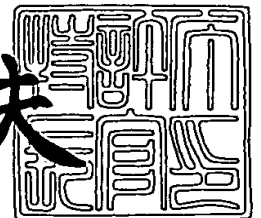
出 願 番 号 特 願 2 0 0 3 - 0 4 6 2 5 1
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 0 4 6 2 5 1]

出 願 人 富 士 通 株 式 会 社
Applicant(s):

2 0 0 3 年 1 1 月 1 0 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 3 - 3 0 9 2 4 0 3

【書類名】 特許願

【整理番号】 0350198

【提出日】 平成15年 2月24日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 19/00

【発明の名称】 セキュリティ管理装置、セキュリティ管理システム、セキュリティ管理方法、セキュリティ管理プログラム

【請求項の数】 10

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内

 【氏名】 面 和成

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内

 【氏名】 鳥居 悟

【特許出願人】

 【識別番号】 000005223

 【氏名又は名称】 富士通株式会社

【代理人】

 【識別番号】 100097250

 【弁理士】

 【氏名又は名称】 石戸 久子

【選任した代理人】

 【識別番号】 100101856

 【弁理士】

 【氏名又は名称】 赤澤 日出夫

【手数料の表示】

【予納台帳番号】 038760

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0014371

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 セキュリティ管理装置、セキュリティ管理システム、セキュリティ管理方法、セキュリティ管理プログラム

【特許請求の範囲】

【請求項 1】 ネットワークにおけるセキュリティに関する情報を提供するセキュリティ情報提供部から取得されるセキュリティ情報と、ネットワークに接続された少なくとも一つのネットワークマシンから取得されるマシン情報とに基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、セキュリティ関連処理の種別とその必要性の有無を判断するセキュリティ診断部と、

前記セキュリティ診断部による診断結果に基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、所定のセキュリティ対策処理を行うセキュリティ実行部とを備えてなるセキュリティ管理装置。

【請求項 2】 請求項 1 に記載のセキュリティ管理装置において、

前記セキュリティ診断部は、さらに、前記ネットワークに接続され、又は前記ネットワークに接続される可能性のあるネットワークマシンについての所定の情報を記憶したマシン関連情報記憶部から得られるマシン関連情報に基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、セキュリティ関連処理の種別とその必要性の有無を判断することを特徴とするセキュリティ管理装置。

【請求項 3】 請求項 2 に記載のセキュリティ管理装置において、

前記マシン関連情報記憶部に記憶されたマシン関連情報は、セキュリティポリシーについて規定した情報であることを特徴とするセキュリティ管理装置。

【請求項 4】 ネットワークに接続された少なくとも一つのネットワークマシンから取得されるマシン情報と、前記ネットワークに接続され、又は前記ネットワークに接続される可能性のあるネットワークマシンについての所定の情報を記憶したマシン関連情報記憶部から得られるマシン関連情報とに基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワ

ークに対して、セキュリティ関連処理の種別とその必要性の有無を判断するセキュリティ診断部と、

前記セキュリティ診断部による診断結果に基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、所定のセキュリティ対策処理を行うためのセキュリティ実行部とを備えてなるセキュリティ管理装置。

【請求項5】 ネットワークにおけるセキュリティに関するセキュリティ情報を提供するセキュリティ情報提供装置と、

前記ネットワークに接続され、又は前記ネットワークに接続される可能性のあるネットワークマシンについての所定の情報を記憶したマシン関連情報データベースと、

前記セキュリティ情報提供部から得られるセキュリティ情報と、前記マシン関連情報データベースから得られるマシン関連情報と、ネットワークに接続された少なくとも一つのネットワークマシンから取得されるマシン情報との少なくともいずれかに基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、被害の有無の判断、または予防の必要性の有無の判断を行う予防システムと、

前記予防システムの判断に基づいて、所定の被害がある場合には修復処理を行い、または予防措置をとる回復システムと

を備えてなるセキュリティ管理システム。

【請求項6】 ネットワークにおけるセキュリティに関するセキュリティ情報を取得するセキュリティ情報取得ステップと、

ネットワークに接続された少なくとも一つのネットワークマシンからマシン情報を取得するマシン情報取得ステップと、

前記セキュリティ情報及び前記マシン情報とに基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、セキュリティ関連処理の種別とその必要性の有無を判断するセキュリティ診断ステップと、

前記セキュリティ診断ステップによる診断結果に基づいて、前記ネットワーク

マシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、所定のセキュリティ対策処理を行うセキュリティ実行ステップと
を備えてなるセキュリティ管理方法。

【請求項 7】 ネットワークに接続された少なくとも一つのネットワークマシンからマシン情報を取得するマシン情報取得ステップと、

前記ネットワークに接続され、又は前記ネットワークに接続される可能性のあるネットワークマシンについての所定の情報を記憶したマシン関連情報記憶部からマシン関連情報を取得するマシン関連情報取得ステップと、

前記マシン情報とマシン関連情報とに基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、セキュリティ関連処理の種別とその必要性の有無を判断するセキュリティ診断ステップと、

前記セキュリティ診断部による診断結果に基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、所定のセキュリティ対策処理を行うためのセキュリティ実行ステップと

を備えてなるセキュリティ管理方法。

【請求項 8】 セキュリティ管理をコンピュータに実行させるセキュリティ管理プログラムであって、

ネットワークにおけるセキュリティに関するセキュリティ情報を取得するセキュリティ情報取得ステップと、

ネットワークに接続された少なくとも一つのネットワークマシンからマシン情報を取得するマシン情報取得ステップと、

前記セキュリティ情報及び前記マシン情報とに基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、セキュリティ関連処理の種別とその必要性の有無を判断するセキュリティ診断ステップと、

前記セキュリティ診断ステップによる診断結果に基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、所定のセキュリティ対策処理を行うセキュリティ実行ステップと

をコンピュータに実行させるセキュリティ管理プログラム。

【請求項 9】 請求項 8 に記載のセキュリティ管理プログラムにおいて、

さらに、前記ネットワークに接続され、又は前記ネットワークに接続される可能性のあるネットワークマシンについての所定の情報を記憶したマシン関連情報記憶部から得られるマシン関連情報を取得するマシン関連情報取得ステップを備え、

前記セキュリティ診断ステップでは、前記セキュリティ情報及び前記マシン情報とともに、前記マシン関連情報に基づいて、前記セキュリティ診断を行うことをコンピュータに実行させるセキュリティ管理プログラム。

【請求項 10】 セキュリティ管理をコンピュータに実行させるセキュリティ管理プログラムであって、

ネットワークに接続された少なくとも一つのネットワークマシンからマシン情報を取得するマシン情報取得ステップと、

前記ネットワークに接続され、又は前記ネットワークに接続される可能性のあるネットワークマシンについての所定の情報を記憶したマシン関連情報記憶部からマシン関連情報を取得するマシン関連情報取得ステップと、

前記マシン情報とマシン関連情報とに基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、セキュリティ関連処理の種別とその必要性の有無を判断するセキュリティ診断ステップと、

前記セキュリティ診断部による診断結果に基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、所定のセキュリティ対策処理を行うためのセキュリティ実行ステップと

をコンピュータに実行させるセキュリティ管理プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、不正アクセスなど、ネットワークシステムに異常をもたらすおそれを排除することができるセキュリティ管理装置、セキュリティ管理システム、セ

セキュリティ管理方法、セキュリティ管理プログラムに関するものである。

【0 0 0 2】

【従来の技術】

従来より、セキュリティ管理サービスのための技術として、例えば以下のよう
なものが知られている。

第1の従来技術は、パッチが適用されるクライアントマシンとクライアントマ
シンに対するパッチデータやソフトウェアデータを保持するサーバコンピュータ
から構成されており、サーバコンピュータがクライアントコンピュータに対して
パッチを適用するというものである（例えば特許文献1，2参照）。

【0 0 0 3】

この動作は以下のように行われる。まず、（1）クライアントコンピュータの
ソフトウェア情報をサーバコンピュータに登録する。（2）次に、依存するソフ
トウェア情報をサーバコンピュータに登録する。そして、（3）クライアントコ
ンピュータに対するソフトウェア更新可否を判定するとともに、（4）パッチを
サーバコンピュータから配信する。

【0 0 0 4】

第2の従来技術は、監視サーバは、監視対象クライアントのウィルスチェック
をリモートから実行しその実行結果を受け取り、ウィルスを検出したときは監視
対象クライアントへウィルス検出を通知するというものである（例えば、特許文
献3参照）。

【0 0 0 5】

この動作は以下のように行われる。まず、（1）監視サーバが監視対象クライ
アントのウィルスチェックの実行／未実行を参照する。（2）監視サーバが未実
行の監視対象クライアントに対してウィルスチェックの実行要求を行う。（3）
監視サーバが実行結果を受け取る。（4）監視サーバが監視対象クライアントへ
ウィルス検出を通知する。

【0 0 0 6】

【特許文献1】

特開 2 0 0 2 - 5 5 8 3 9 号公報

【特許文献 2】

特開 2000-250743 号公報

【特許文献 3】

特開平 11-327897 号公報

【0007】**【発明が解決しようとする課題】**

しかしながら、第 1 の従来技術では、Web で公開されている様々なセキュリティ情報をマシン情報に応じて選別取得する機能がなく、セキュリティ対策の柔軟性に乏しく、幅広い適用が困難である。同様に第 2 の従来技術でも、ウィルスチェックのみに限定され、マシン情報に応じた様々なセキュリティ対策を講じることが不可能である。

【0008】

なお、本出願人は、パッチが公開されていないセキュリティホールに対してフィルタリングルール作成し、パッチが公開されるまでフィルタによって防御し、パッチが公開されると前記ルールが削除されるようにした技術を提案しているが、かかる技術においても、ネットワークマシンのマシン情報を取得して、マシンに合わせたルールを作成する機能がなく、やはり幅広い適用性に劣る。

【0009】

本発明は、上述した課題に鑑みてなされたものであり、ネットワークを構成するネットワークマシンからマシン情報を取得し、このマシン情報を参照しつつ種々のセキュリティ対策を講じることができ、もって柔軟性に優れ、幅広く適用することが可能なセキュリティ管理装置、セキュリティ管理システム、セキュリティ管理方法、セキュリティ管理プログラムを提供することを目的とする。

【0010】**【課題を解決するための手段】**

上述した課題を解決するため、本発明は、ネットワークにおけるセキュリティに関する情報を提供するセキュリティ情報提供部から取得されるセキュリティ情報と、ネットワークに接続された少なくとも一つのネットワークマシンから取得されるマシン情報とに基づいて、前記ネットワークマシン若しくは前記ネットワ

ークマシンが含まれる所定のネットワークに対して、セキュリティ関連処理の種別とその必要性の有無を判断するセキュリティ診断部と、前記セキュリティ診断部による診断結果に基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、所定のセキュリティ対策処理を行うセキュリティ実行部とを備えてなるものである。

【0011】

また、本発明のセキュリティ管理装置において、前記セキュリティ診断部は、さらに、前記ネットワークに接続され、又は前記ネットワークに接続される可能性のあるネットワークマシンについての所定の情報を記憶したマシン関連情報記憶部から得られるマシン関連情報に基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、セキュリティ関連処理の種別とその必要性の有無を判断することを特徴とする。

【0012】

また、本発明のセキュリティ管理装置において、前記マシン関連情報記憶部に記憶されたマシン関連情報は、セキュリティポリシーについて規定した情報であることを特徴とする。

【0013】

なお、本発明のセキュリティ管理装置において、前記セキュリティポリシーは、所定のマシン情報についてのフィルタリング防御又は通信制御について規定し、前記セキュリティ実行部はフィルタリング処理又は通信制御を実行することを特徴とすることができる。

また、本発明のセキュリティ管理装置において、前記セキュリティポリシーは、所定のプログラムについてのパッチ適用又はワクチン投与について規定し、前記セキュリティ実行部は前記所定のプログラムにパッチ適用処理又はワクチン投与処理を実行することを特徴とすることができる。

さらに、本発明のセキュリティ管理装置において、前記セキュリティ実行部によるセキュリティ対策処理が実行された場合に、その実行結果における前記ネットワークマシン若しくはネットワークにおける動作確認が行われることを特徴とすることができる。

【0014】

また、本発明のセキュリティ管理装置において、前記セキュリティ実行部によるセキュリティ対策処理が実行された場合において、そのセキュリティ対象についてフィルタリングルールが設定されている場合は、そのルールの削除が行われることを特徴とすることができる。

さらに、本発明のセキュリティ管理装置において、さらに新規に導入されるネットワークマシンからの接続要求を受け付ける接続要求受付部を備え、前記セキュリティ診断部は、前記接続要求受付部により新規ネットワークマシンからの接続要求を受け付けた場合に、前記マシンを離隔状態として該ネットワークマシンにアドレスを与え、前記マシン情報と前記セキュリティ情報とに基づいて、前記セキュリティ関連処理として前記ネットワークマシンに対する離隔解除を行うか否かを判断することを特徴とすることができる。

【0015】

また、本発明のセキュリティ管理装置において、さらに新規に導入されるネットワークマシンからの接続要求を受け付ける接続要求受付部を備え、前記セキュリティ診断部は、前記接続要求受付部により新規ネットワークマシンからの接続要求を受け付けると共に、前記ネットワークマシンからマシン情報を受け付けると、該マシン情報と前記セキュリティ情報とに基づいて、前記セキュリティ関連処理として前記ネットワークマシンに対するアドレス付与の可否を判断することを特徴とすることができる。

【0016】

また、本発明のセキュリティ管理装置は、ネットワークに接続された少なくとも一つのネットワークマシンから取得されるマシン情報と、前記ネットワークに接続され、又は前記ネットワークに接続される可能性のあるネットワークマシンについての所定の情報を記憶したマシン関連情報記憶部から得られるマシン関連情報とに基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、セキュリティ関連処理の種別とその必要性の有無を判断するセキュリティ診断部と、前記セキュリティ診断部による診断結果に基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含

まれる所定のネットワークに対して、所定のセキュリティ対策処理を行うためのセキュリティ実行部とを備えてなるものである。

【0017】

本発明のセキュリティ管理装置において、前記マシン関連情報は、コンピュータウィルスの挙動内容を示す情報を含み、前記マシン情報には所定のファイルのハッシュ値、ウィルススキャン結果の少なくともいずれか一つを含み、前記セキュリティ診断部は、所定のネットワークマシンについて、離隔する必要性の有無を判断し、前記セキュリティ実行部は前記セキュリティ診断部により前記ネットワークマシンを離隔する必要性があると判断された場合には、前記ネットワークマシンを離隔するための処理を行うことを特徴とすることができる。

【0018】

また、本発明のセキュリティ管理装置において、前記ネットワークマシンの通信を監視するネットワーク監視部を備え、前記マシン関連情報は、ネットワークマシンのプロファイルに関する情報であり、前記セキュリティ診断部は、前記ネットワーク監視部からの監視情報と前記マシン情報と前記ネットワークマシンのプロファイルに関する情報とに基づいて、所定のネットワークマシンについて、離隔する必要性の有無を判断し、前記セキュリティ実行部は前記セキュリティ診断部により前記ネットワークマシンを離隔する必要性があると判断した場合には、前記ネットワークマシンを離隔するための処理を行うことを特徴とすることができる。

【0019】

また、本発明のセキュリティ管理装置において、前記セキュリティ診断部は、被害範囲の同定を行い、離隔範囲を定めることを特徴とすることができる。

さらに、本発明のセキュリティ管理装置において、前記セキュリティ診断部の診断結果に基づき、所定の被害を受けたネットワークマシン若しくはネットワークに対して修復を行うための修復部が備えられていることを特徴とすることができる。

【0020】

また、本発明のセキュリティ管理装置において、被害修復が行われた場合、離

隔を解除する離隔解除部が備えられていることを特徴とすることができる。

また、本発明のセキュリティ管理装置において、前記マシン情報は、機器構成の変更の通知と、少なくともその変更される機器構成の情報を含み、前記マシン関連情報は、前記ネットワークにおいて使用の可否を規定した機器構成情報を含むことを特徴とすることができる。

さらに、本発明のセキュリティ管理装置において、前記セキュリティ診断部は、前記ネットワークマシンの離隔の必要性について判断し、セキュリティ実行部は前記セキュリティ診断部の判断結果に基づいて前記ネットワークマシンを離隔するための処理を行うことを特徴とするものである。

【0021】

また、本発明のセキュリティ管理システムは、ネットワークにおけるセキュリティに関するセキュリティ情報を提供するセキュリティ情報提供装置と、前記ネットワークに接続され、又は前記ネットワークに接続される可能性のあるネットワークマシンについての所定の情報を記憶したマシン関連情報データベースと、前記セキュリティ情報提供部から得られるセキュリティ情報と、前記マシン関連情報データベースから得られるマシン関連情報と、ネットワークに接続された少なくとも一つのネットワークマシンから取得されるマシン情報とに基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、被害の有無の判断、または予防の必要性の有無の判断を行う予防システムと、前記予防システムの判断に基づいて、所定の被害がある場合には修復処理を行い、または予防措置をとる回復システムとを備えてなる。

【0022】

本発明のセキュリティ管理システムにおいて、前記予防システム又は前記回復システムは複数設けられ、これらシステムを統括的に管理する管理センタが設けられていることを特徴とすることができる。

また、本発明のセキュリティ管理システムにおいて、前記予防システム又は前記回復システムは複数設けられ、これら複数のシステムのそれぞれで取得された情報が互いに共有されることを特徴とすることができる。

さらに、本発明のセキュリティ管理システムにおいて、前記セキュリティ情報

提供部の所有者側に前記予防システム及び前記回復システムが設けられていることを特徴とすることができる。

【0023】

また、本発明のセキュリティ管理システムにおいて、前記セキュリティ情報提供部の所有者側に前記予防システムが設けられ、管理サービスを提供する管理サービス提供者側に前記回復システムが設けられることを特徴とすることができる。

さらに、本発明のセキュリティ管理システムにおいて、管理サービスを提供する管理サービス提供者側に前記予防システム及び前記回復システムが設けられることを特徴とすることができる。

また、本発明のセキュリティ管理システムにおいて、前記回復システムにおいて取得された所定の情報が新たなセキュリティ情報として、前記予防システムにフィードバックされることを特徴とすることができる。

【0024】

また、本発明のセキュリティ管理方法は、ネットワークにおけるセキュリティに関するセキュリティ情報を取得するセキュリティ情報取得ステップと、ネットワークに接続された少なくとも一つのネットワークマシンからマシン情報を取得するマシン情報取得ステップと、前記セキュリティ情報及び前記マシン情報とに基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、セキュリティ関連処理の種別とその必要性の有無を判断するセキュリティ診断ステップと、前記セキュリティ診断ステップによる診断結果に基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、所定のセキュリティ対策処理を行うセキュリティ実行ステップとを備えてなるものである。

【0025】

本発明のセキュリティ管理方法において、さらに、前記ネットワークに接続され、又は前記ネットワークに接続される可能性のあるネットワークマシンについての所定の情報を記憶したマシン関連情報記憶部から得られるマシン関連情報を取得するマシン関連情報取得ステップを備え、前記セキュリティ診断ステップで

は、前記セキュリティ情報及び前記マシン情報とともに、前記マシン関連情報に基づいて、前記セキュリティ診断を行うことを特徴とすることができる。

【0026】

また、本発明のセキュリティ管理方法は、ネットワークに接続された少なくとも一つのネットワークマシンからマシン情報を取得するマシン情報取得ステップと、前記ネットワークに接続され、又は前記ネットワークに接続される可能性のあるネットワークマシンについての所定の情報を記憶したマシン関連情報記憶部からマシン関連情報を取得するマシン関連情報取得ステップと、前記マシン情報とマシン関連情報とに基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、セキュリティ関連処理の種別とその必要性の有無を判断するセキュリティ診断ステップと、前記セキュリティ診断部による診断結果に基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、所定のセキュリティ対策処理を行うためのセキュリティ実行ステップとを備えてなるものである。

【0027】

また、本発明は、セキュリティ管理をコンピュータに実行させるセキュリティ管理プログラムであって、ネットワークにおけるセキュリティに関するセキュリティ情報を取得するセキュリティ情報取得ステップと、ネットワークに接続された少なくとも一つのネットワークマシンからマシン情報を取得するマシン情報取得ステップと、前記セキュリティ情報及び前記マシン情報とに基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、セキュリティ関連処理の種別とその必要性の有無を判断するセキュリティ診断ステップと、前記セキュリティ診断ステップによる診断結果に基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、所定のセキュリティ対策処理を行うセキュリティ実行ステップとをコンピュータに実行させるものである。

【0028】

また、本発明のセキュリティ管理プログラムにおいて、さらに、前記ネットワークに接続され、又は前記ネットワークに接続される可能性のあるネットワーク

マシンについての所定の情報を記憶したマシン関連情報記憶部から得られるマシン関連情報を取得するマシン関連情報取得ステップを備え、前記セキュリティ診断ステップでは、前記セキュリティ情報及び前記マシン情報とともに、前記マシン関連情報に基づいて、前記セキュリティ診断を行うことをコンピュータに実行させるものである。

【0029】

また、本発明は、セキュリティ管理をコンピュータに実行させるセキュリティ管理プログラムであって、ネットワークに接続された少なくとも一つのネットワークマシンからマシン情報を取得するマシン情報取得ステップと、前記ネットワークに接続され、又は前記ネットワークに接続される可能性のあるネットワークマシンについての所定の情報を記憶したマシン関連情報記憶部からマシン関連情報を取得するマシン関連情報取得ステップと、前記マシン情報とマシン関連情報とに基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、セキュリティ関連処理の種別とその必要性の有無を判断するセキュリティ診断ステップと、前記セキュリティ診断部による診断結果に基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、所定のセキュリティ対策処理を行うためのセキュリティ実行ステップとをコンピュータに実行させるものである。

【0030】

【発明の実施の形態】

以下に、本発明の実施の形態を図面を用いて説明する。

図1は、本発明の実施の形態におけるセキュリティ管理システムの全体構成を原理的に示すブロック図、図2は予防システムの全体構成をより詳細に示すブロック図である。本実施の形態では、ネットワーク1内に接続され、ネットワークを構成するネットワークマシン2と、各種情報を提供する情報提供装置3と、ネットワーク1（図4参照）内のネットワークマシン2に対するセキュリティ対策を講じるためめ予防システム4と、予防システム4と協働して、セキュリティ対策の一部を実行するため、例えばネットワーク1若しくはネットワークマシン2の隔離を行い、或いはそれを解除し、更には必要に応じて被害を受けたネットワ

ーク 1 若しくはネットワークマシン 2 を回復させるための回復システム 5 とを備えて構成される。

【0031】

なお、図 1 に示す情報提供装置 3、予防システム 4、及び回復システム 5 はネットワークマシン 2 と同様、インターネットやその他の通信回線を介して相互に接続され得、また、各システムは通常の各種判断、処理を行うことができるコンピュータ（例えば PC）を備えている。ここでは、例えば、ネットワークマシン 1 は DNS (Domain Name System) サーバやメールサーバを想定しており、情報提供装置 3 は Web ページにおいて無償でセキュリティホール情報やパッチ関連情報等を公開しているものとする。情報提供装置 3 は従来と変らない方式で情報を公開しており、必要に応じて暗号化通信を行うものとする。また、従来のシステムに予防システム 4、回復システム 3 を導入することにより、セキュリティ管理システムによるサービスを開始できる。予防システム 4 及び回復システム 5 の導入方法は、購入若しくはレンタルとする。

【0032】

予防システム 4 は、図 2 に示されるように、セキュリティ関連処理の種別とその必要性の有無を判断する診断部（セキュリティ診断部）41 と、各種データベース 42 と、ネットワークマシン 2 を含むネットワーク 1 の状態を監視するネットワーク監視装置 43 と、診断部 41 の診断結果に基づいて、例えば回復システム 5 に予防処置の指示を行う予防実行部 44 とを備えている。

診断部 41 は、必要に応じてネットワークマシン 2、情報提供装置 3、各種データベース 42、及びネットワーク監視装置 43 からの情報を取得する情報取得部 411 と、情報取得部 411 で得られる情報を検索し、或いは比較する情報検索／比較部 412 と、情報検索／比較部 412 での各種情報の比較結果に基づいて、セキュリティ関連処理の種別とその必要性の有無についての判定を行う判定部 413 とを備えて構成されている。

以下、これらの構成を基本構成として、各種動作を実施の形態に対応させて説明する。なお、実施の形態における予防システムは本発明のセキュリティ管理装置に対応している。

【 0 0 3 3 】

実施の形態 1.

図 3 は実施の形態 1 を示すブロック構成図、図 4 はセキュリティ管理が実施されるネットワークを示すブロック図、図 5 は実施の形態 1 の動作を示すフローチャートである。

実施の形態 1 は、情報提供装置により公開されたセキュリティホール情報に基づいてセキュリティ対策を行うようにした場合について説明する。

未公表なものも含まれるセキュリティホール情報が情報提供装置 3 A により公開された場合（ステップ S 0）、予防システム 4 A の情報取得部 4 1 1（図 2）はセキュリティホール情報（セキュリティホール番号、対象 OS 名、対象サービス、脆弱性内容等）3 a を情報提供装置 3 A からダウンロードし（ステップ S 1）、当該セキュリティ情報が正当な情報であるかどうかを検証し（ステップ S 2）、正当な情報だけを取り入れる（ステップ S 2、YES）。

【 0 0 3 4 】

このセキュリティ情報が正当なものであるか否かの検証は、例えば、情報自体の信憑性に基づいて行われ、予め発信元の信頼性によりレベル分けを行っておき、所定のレベル以上の信頼性があるとされた発信元からの情報を用いるようにする。また、実際に、実験器具を用いて信頼性を確認することもできる。例えば、実験的に Web サーバを立ち上げておき、特定の文字列や命令を含み、セキュリティホール情報に該当する状態を作り上げて実証することが行われる。或いは、検証を行う他の方法として、情報自体の正当性（情報が改ざんされていないかどうか）のチェックを行うことによっても行い得る。例えば、付加されている電子署名を検証したり、付加されているハッシュ値を検証することによって行い得る。

【 0 0 3 5 】

また、予防システム 4 A（診断部 4 1 A）は、ネットワーク 1 内のマシン情報（マシン名、IP アドレス、アーキテクチャ名、OS 名、インストールされたパッケージ群等）2 a を取得し（ステップ S 3）、当該正当なセキュリティ情報と比較照合することでセキュリティホールがあるマシンの存在を判定し、存在する

場合はそのマシンを選択する（ステップ S 4）。なお、マシン情報の一例を図 17 に示している。次に、情報提供装置 3 からの情報に当該セキュリティホールの緊急度が高い旨の情報が含まれている場合は、その情報を考慮し、直ちに各種サーバ 42 のうちから、フィルタリングデータベース 42 A を参照して、フィルタリング防御を行うことについて規定されているか否か（フィルタリングデータベースの登録項目にマッチするか否か）を検索して判断し（ステップ S 5）、防御する必要があると判断された場合、対象となるマシンのマシン情報と脆弱性内容をフィルタリングルール作成装置 441 に送信する。フィルタリングデータベースはフィルタリングルールの設定についてのセキュリティポリシーを規定したデータベースである。なお、予防システム 4 A は、フィルタリングルールの作成に所定時間以上要する場合は、脆弱対象となるソフトウェアを取り敢えず停止させるように指示することもできる。

【0036】

そして、取得した情報を元にフィルタリングルール作成装置 441 はルール番号と対応セキュリティホール番号を含む新規のフィルタリングルール 441 a を作成し（ステップ S 6）、ルール実行部 443 は、そのルールによってセキュリティホールへのアタックを防御する（ステップ S 7）。またフィルタリングルール作成装置 441 は、その作成された新規ルールをルールデータベース 442 に登録する（ステップ S 8）。本実施の形態におけるフィルタリングルール作成装置 441 は、セキュリティホール情報 3 a に該当するネットワークマシンについて、搭載されるソフトウェア“SUNwftpu”に不正文字列「x x x」の情報が送信される場合を防止するよう、新規ルールを作成し、ルールデータベース 442 に新規ルールを登録する。

【0037】

そして、ルール実行部 443 は、ルールデータベース 442 に登録されたルールに基づいて、そのような情報が当該ネットワークマシンに到達するのを防止する。この場合、回復システム 5（図 2）は、ルール実行部 443 からの指示を受け、例えば、図 4 に示すネットワークにおいて、ルール設定されたネットワークマシンに不正文字列が外部より送信されてきた場合に、防御装置 11 を動作させ

てそれを遮断させる。なお、図4に示されるネットワークは、複数のネットワークセグメント1A～1Dに離隔装置12～15を介して分割されている。ネットワークの入り口には、防御装置11（ファイアウォール）が設けられ、また、防御装置11を介してインターネットINと接続可能なDMZ (Demilitarized Zone) が構築されている。

【0038】

以上、実施の形態1ではセキュリティ関連処理の種別の一例としてフィルタリングルールの作成について説明したが、通信機器として動作するネットワークマシンに対しては、通信制御のルールを作成して設定するようにしても良い。この通信制御には、例えば到着通信データの流量制御及び発呼制御、ルーティング情報の変更等が挙げられる。

【0039】

なお、実施の形態1においては、フィルタリングルール作成装置441、ルールデータベース442及びルール実行部443が図2に示した予防実行部44を構成している。

【0040】

実施の形態2.

図6は実施の形態2を示すブロック構成図、図7は実施の形態2の動作を示すフローチャートである。

実施の形態2は、情報提供装置により公開されたパッチ関連情報に基づいてセキュリティ対策を行うようにした場合について説明する。

【0041】

予防システム4Bの診断部41Bは、情報提供装置3Bから新たなパッチが公開されると（ステップS10）、当該パッチファイルとそのパッチ関連情報（対象セキュリティホール番号、アーキテクチャ名、対象OS名、対象サービス）3bを情報提供装置3Bからダウンロードし（ステップS11）、ネットワークマシン2からマシン情報（マシン名、IPアドレス、アーキテクチャ名、OS名、インストールされたパッケージ群、適用済みパッチ群等）2bを取得し（ステップS12）、それらを比較照合することでパッチを充てる必要があるマシンの存

在を判定し、そのマシンを選択する（ステップS13）。

【0042】

次に、パッチ適用データベース42Bを参照しながらパッチを充てることに規定（若しくはパッチを充てることに禁止項目）があるかどうかを判断し（ステップS14）、充てることが問題ないと判断された場合（ステップS14、YES）、診断部41Bからの指示に基づいてパッチ適用部451が対象マシンにパッチを適用し（ステップS15）、それと同時に、ルール実行部443で実行されるフィルタリングルールがルールデータベース452に登録されている場合は、当該パッチに関連するフィルタリングルール41bを削除する（ステップS16）。

【0043】

パッチ適用後は、パッチ適用に係るマシンの動作がパッチ適用前と変らないことを確認するため、マシンの動作確認を行う。この確認は、診断部41Bにおいて、マシン情報の関連情報として動作情報を取得することで行うようにしても良いし、或いは図1、図2に示した回復システム、若しくは図2に示したネットワーク監視装置で行うようにしても良い。この確認方法の具体例としては、例えば次のようなものが挙げられる。

【0044】

（1）プロセスの確認

これは、例えばソフトウェアが起動しているかどうかを判断することによって行われる。

（2）サービスやソフトウェアを利用しての確認

これは、例えばWebサーバならばページが表示されているか否かを判断することによって行うことができる。また、メールサーバならばメールが送受信されているか否かを判断することによって行うことができる。

（3）固有設定の確認

これは、例えばファイアウォールならパケットを拒否できているか否かを判断することによって行うことができる。また、メールサーバならば不正中継が行われているか否かを判断することによって行うことができる。

(4) その他の確認

例えば、マシンのプロファイル（後述の実施の形態3で説明）を用いて動作確認を行うことで行われる。例えば、プロファイルを保存したデータベースを用意しておくと共に、過去の所定期間（例えば一ヶ月）のコンピュータプロセスやネットワークのログをプロファイルデータベースに保存しておき、パッチ適用後に取得したログと比較して相違点をチェックすることにより判断する。

【0045】

以上の確認において、マシン動作が異常と判断されると、回復システム、或いはパッチ適用部451はパッチを排除する処理を行う。

以上の構成において、パッチ適用部451とルールデータベース、及びルール実行部443からなる予防実行部44Bは、図2における予防実行部44に相当する。

【0046】

実施の形態3.

図8は実施の形態3を示すブロック構成図、図9は被害の有無を判断する動作を示す概念図、図10は実施の形態3の動作を示すフローチャートである。

実施の形態3は、ネットワークマシンの通信ログや挙動に基づいて被害の有無を判断して、そのセキュリティ対策を行うようにした場合について説明する。

【0047】

実施の形態3において診断部41Cは、ネットワーク監視装置43において、通信またはマシンの挙動を監視して（ステップS20）、監視内容から送信元IPアドレスや送信先IPアドレス、不正通信の種類および対象サービス等の情報等の通信ログ43aを取得し（ステップS21）、ネットワークマシン2からは対象ファイルのハッシュ値やウィルススキャン結果等の診断情報をマシン情報2cとして取得する（ステップS22）。そして、それらをアタック（バックドア）／ウィルスデータベース421に登録されているウィルス等の挙動内容、シグネチャ等と比較照合し、或いはマシンプロファイルデータベース422に登録されている通信プロファイルやプロセスプロファイルと比較照合して被害を受けているか否かを判断する（ステップS23）。被害を受けていると判断された場合

(ステップS 23、YES)は、被害の拡散性があるか否かを判断する(ステップS 24)。この被害の拡散性の判断は、被害を受けているマシンや被害規模の推定とともに行われ、例えば被害を受けているマシンの数若しくは範囲の経時変化を監視することにより判断することができる。拡散性があると判断された場合(ステップS 24、YES)は、その被害範囲の同定が行われる(ステップS 25)。

【0048】

そして、被害に拡散性が有ると判断された場合、診断部41Cは、各ネットワークマシンからネットワーク情報(マシンの配置情報、ネットワーク構成、離隔点のIPアドレス等)をマシン情報として取得し、その離隔点を決定し、その離隔指示のための離隔情報(アタック元のIPアドレス、アタック元のMACアドレス、遮断すべき通信の種類等)41cを離隔/解除/修復指示部(予防実行部)44Cに送出する(ステップS 26)。なお、ここで、離隔とはネットワークマシンからの送信を規制する意味であり、更にこの場合、所定の通信(相手先、データ量)のみを許可したり、許可されていない送信先への通信を不正通信として遮断することなどが含まれる。離隔点は、図4の例においては、離隔装置を特定することにより定められる。

【0049】

離隔情報を受けた離隔/解除/修復指示部(予防実行部)44Cは回復システム5に離隔情報に基づく離隔指示を送信する。回復システム5は、離隔点となるルータ(離隔装置12~15)に離隔動作を行うよう指示を通知する。この回復システム5からの指示によりルータは離隔点における通信の制限を行う。この通信制御は例えばネットワーク監視装置43により監視され、診断部41Cでは、取得される通信ログ等に基づき、離隔できたことが図示しない確認部により確認される。その後、回復システム5は、所定の被害については、被害を受けたマシンの修復を行うことができる。また、そのような被害が発生した場合には、それをユーザに通知する構成とすることもできる。また、診断部41Cは、新たな被害をもたらした現象等についてその不正シグネチャ等をアタック/ウィルスデータベース421に保存する(ステップS 27)。このデータベース421に保存

された新たな情報は、例えば通信回線を介して他のネットワークにおけるセキュリティを管理する情報提供装置や予防システムに提供されることができ、予防対策を迅速に講じるための情報として使用され得る。

【0050】

回復システム5により行われる修復には、例えば被害を受けてレジスタ等の設定値が変更された場合に、被害を受ける前の正常な状態（例えばデフォルト値）に戻すような処理が含まれる。また、パッチの未適用部分が判断された場合は、その部分に対しては新たにパッチ適用を行う処理も含まれる。更には、被害を受けた或いは被害の原因となるファイルを削除したり、システムを再起動すること、また、バックアップファイルを用いてもとの状態に戻す（再インストールする）ようなことも行い得る。

【0051】

なお、被害に拡散性がないと判断された場合（ステップS24、NO）には、その修復或いはその表示のため、診断部41Cは離隔／解除／修復指示部（予防実行部）44Cにその被害情報を送出し（ステップS28）、離隔／解除／修復指示部44Cは修復指示を回復システム5に送信する。回復システム5は被害の修復を行える場合は、その修復を行う。また、ネットワークマシン2の所有者側に通知を行い、その旨を知らせる。

【0052】

図9は異常の有無を判断することで被害の有無を判断するための動作をより詳細に示すための図である。例えば、既知のウイルスによる場合は、アタック／ウイルスデータベース421に格納されている情報と通信ログ43aとから通信内容の異常を判断できる。図9の場合は、例えば不正シグネチャとして“xxx”が通信内容43a-2におけるマシン名「Srv01」のマシンに表れている。これにより、当該マシンがウイルスによる被害を受けていると判断することができる。また、この通信内容の履歴により、被害を受けているマシンが時間と共に増えている場合は拡散性があるものと判断できる。さらに、既知でないウイルス等による被害については、やはり、通信内容の履歴をマシンプロファイルデータベース422に格納されている正常通信プロファイルと照合することにより、正常

通信プロファイルと異なる履歴が観察される場合に、何らかの被害を受けていると判断することもできる。この判断基準は、例えば所定期間においてなされた全ての通信（送信）における各接続先アドレスの配分比率 4 3 a-1 と、正常なプロファイルにおけるその配分比率 4 2 2 との差異を定量化する規定を作成し、その差異が所定値よりも大きくなったときに異常を判断するようにして定めることができる。

【0053】

図 9 においては、これらの配分比率が異なっているため、その比較の対象となったマシンに異常が発生していると判断することができる。また、通信内容の履歴より、そのような異常を有するマシンが増えていると判断されるとその被害は拡散性を有すると判断できるため、そのマシンに対する離隔情報が診断部より送出される。この離隔情報には、例えば当該マシン若しくはそのマシンを含むネットワークセグメントからの全ての送信を遮断する完全遮断モードと、不正シグネチャだけを抑えるドロップモードと、通信量を制限する通信量制限モードとが用意されている。

【0054】

このようにして、実施の形態 3 においては、既知の攻撃（バックドア）、ウィルスのネットワーク（マシン）への攻撃のみならず、未知の攻撃からもネットワーク（マシン）への攻撃に対する防御を行うことができる。また、未知の攻撃に対して取得された情報を他のネットワークにおけるセキュリティシステムでも使用可能とすることができる。

【0055】

なお、実施の形態 3 においては、離隔／解除／修復指示部 4 4 C が図 2 に示した予防実行部 4 4 を構成している。

【0056】

実施の形態 4.

図 1 1 は実施の形態 4 を示すブロック構成図、図 1 2 は実施の形態 4 の動作を示すフローチャートである。

実施の形態 4 は、新たなネットワークマシン 2 が接続される場合について説明

する。

実施の形態 4 においては、セキュリティ管理対象となるネットワークに新たなネットワークマシン 2 が接続されると、当該ネットワークマシン 2 の付与予定 IP アドレスや当該ネットワークマシン 2 の MAC アドレスによって、とりあえず、そのネットワークマシン 2 を含むネットワークが最も小さいセグメントで隔離される。しかる後に当該マシン 2 に IP アドレスが与えられる。そして、そのマシンに対しての予防が実行され、若しくは安全性が確認され、ネットワークにおけるそのマシン 2 の安全性が確保された後、当該マシン 2 の隔離が解除されるようにしたものである。

【0057】

すなわち、予防システム 4 D は、新たなネットワークマシン 2 がネットワークに設置されると、その接続要求を受け付ける接続要求受付部 4 5 を備え、接続要求がなされると（ステップ S 3 1）、診断部 4 1 D は隔離／解除指示部 4 4 D を介して回復システム 5 により隔離を実行する（ステップ S 3 2）。回復システム 5 は新たなネットワークマシン 2 が管轄下となる、図 4 に示したいずれかの隔離装置を動作させて隔離を行う。隔離が実行されると、診断部 4 1 D は、そのマシンの IP アドレスやマックアドレスを付与する（ステップ S 3 3）。IP アドレス等が付与されると、診断部 4 1 D は、情報提供装置 3 D からセキュリティ情報 3 d として、セキュリティホール情報やパッチ関連情報を取得し（ステップ S 3 4）、また、ネットワークマシン 2 からマシン情報 2 d を取得し（ステップ S 3 5）、安全性を確保する。

【0058】

この動作は、実施の形態 1 や実施の形態 2 で示したものと同一である。即ち、マシン情報に情報提供装置から得られるセキュリティホール情報やパッチ関連情報に該当するものがあれば（ステップ S 3 6、YES）、フィルタリングデータベース（図 1 の 4 2 A）やパッチ適用データベース（図 6 の 4 2 B）を検索し、適宜フィルタリングルールを作成したり、パッチ適用を行うよう動作し、その予防を行う（ステップ S 3 7）。このようにして、新たなネットワークマシンの安全性が確保されると、或いは当該マシンがセキュリティホール情報やパッチ関連

情報に該当することが無く、安全性を確保する必要性がないと判断された場合（ステップS 36、NO）は、その時点で離隔／解除指示部44Dにより離隔解除指示を出させ（ステップS 38）、回復システム5により離隔動作をさせていた離隔装置の離隔動作を解除させる。

【0059】

実施の形態4においては、離隔／解除指示部44Dが図2に示した予防実行部44を構成している。

【0060】

実施の形態5.

図13は実施の形態5を示すブロック構成図、図14は実施の形態5の動作を示すフローチャートである。

実施の形態5は、接続されようとするネットワークマシン2Eに、例えばブロードキャストを利用するなど、IPアドレスがない状態でマシン情報を送信する機能がインストールされている場合について説明する。

【0061】

実施の形態5においては、当該新たなネットワークマシン2Eがセキュリティ管理対象のネットワークに接続された場合に、予防システム4Eは、当該マシン2Eからマシン情報を取得し、情報提供装置3Eからセキュリティ情報（セキュリティホール情報、パッチ関連情報等）をダウンロードし、予防の必要性の有無を判断する。そして、予防の必要性が無いと判断された場合に、初めてIPアドレスを付与し、当該ネットワークマシンの接続を許可する。

【0062】

即ち、予防システム4Eは、接続要求受付部45と接続可否指示部46とを備え、接続要求受付部45がネットワークマシン2Eからの接続要求を受け付ける（ステップS 40）と共に、診断部41Eがネットワークマシン2Eからのマシン情報2eを取得すると（ステップS 41）、診断部41Eは、情報提供装置3Eからセキュリティ情報3eを取得し（ステップS 42）、マシン情報2eと比較する。そして安全性が高く予防の必要性なしと判断された場合（ステップS 43、NO）、初めてIPアドレスを付与する（ステップS 44）。

【 0 0 6 3 】

一方、安全性が高くなく、予防の必要性があると判断された場合（ステップ S 4 3， Y E S）は、 I P アドレスは付与されない（ステップ S 4 5）。なお、この場合は、実施の形態 4 の動作に移ることにより、予防処理が行われて I P アドレスが付与される。

【 0 0 6 4 】

なお、この場合のネットワークマシン 2 E の構成は、ネットワークに接続されたことを判断する接続判断部 2 1 と、接続判断部 2 1 により接続が判断された場合に、自己の情報をマシン情報として収集して取得するマシン情報取得部 2 2 と、マシン情報取得部 2 2 により取得された情報を接続要求と共に予防システム 4 E（診断部 4 1 E）に送信するマシン情報送信部 2 3 とを備えて構成される。

このように、実施の形態 5 では、ネットワークマシンに I P アドレスがない状態でマシン情報を送信する機能がインストールされている場合には、その安全性を確保した後で I P アドレス等を付与して接続を許可することでネットワークの安全性が確保される。

【 0 0 6 5 】

実施の形態 5 においては、接続可否指示部 4 6 が図 2 に示した予防実行部 4 4 を構成している。

【 0 0 6 6 】

実施の形態 6 .

図 1 5 は実施の形態 6 を示すブロック構成図、図 1 6 は実施の形態 6 の動作を示すフローチャートである。

実施の形態 6 は、ネットワークマシン 2 の構成が変更された場合に、その変更が行われたこと機器構成変更通知として送信する機能が当該ネットワークマシンにインストールされている場合について説明する。

【 0 0 6 7 】

このようなネットワークマシン 2 F においてその構成変更が行われると、ネットワークマシン 2 F は、機器構成変更通知を診断部 4 1 F に送信する（ステップ S 5 0）。診断部 4 1 F では、その機器構成変更通知を受けるとネットワークマ

シン 2 F から機器を構成する情報として機器構成情報 2 f を受け取ると共に、ネットワーク内のマシンにおいて使用許可されている機器構成（部品を含む）について、予め登録されている機器構成データベース 4 2 F からその構成情報を読み出し（ステップ S 5 1）、比較照合して使用許可されている機器構成であるか否かを検証する（ステップ S 5 2）。

【0068】

許可されている構成であれば、そのまま離隔することなく、処理を終了する。一方、許可されていない構成が含まれている場合は、離隔を行う（ステップ S 5 3）。この離隔処理は例えば、離隔／解除指示部 4 4 F を介して回復システム 5 F に離隔処理を行うように通知することで行われる。なお、本実施の形態では、許可された機器構成でないことが判断された時点で離隔を行うようにしたが、機器構成変更通知があった時点（ステップ S 5 0）において直ちに離隔を行い、許可された構成であることが判断された（ステップ S 5 2）後に、離隔を解除する構成としても良い。

【0069】

実施の形態 6 によれば、ネットワークマシンの構成変更により生じる被害を予防することができる。なお、機器構成情報 2 f には、例えば、マシン名、DVD／CD-ROM、ネットワークアダプタ、フレキシブルディスク、PS/2 マウス、USB フラッシュメモリ等が含まれている。また、ここでの構成変更には、構成部品の追加のみならず、取り外す場合も含まれる。

【0070】

実施の形態 6 においては、離隔／解除指示部 4 4 F が図 2 に示した予防実行部 4 4 を構成している。

【0071】

実施の形態 7.

図 1 8 は本発明の実施の形態 7 として、各システムの第 1 の配属構成を示している。

図 1 8 に示す例では、情報サービス提供者（情報提供装置 3 を有する者）7 0 が予防システム 4 と回復システム 5 を有し、管理サービス提供者 7 1 と一体にな

っている。情報サービス提供者 70 は顧客ネットワーク 72 からシステム情報（顧客のネットワークの情報）10 を取得し、独自のセキュリティ情報を用いて顧客ネットワーク 72 毎にパッチおよびフィルタリングルール 30 を提供する。

【0072】

実施の形態 8.

図 19 は本発明の実施の形態 8 として、各システムの第 2 の配属構成を示している。

図 19 に示す例では、情報サービス提供者 70 が予防システム 4 を有し、管理サービス提供者 71 が回復システム 5 を有する。管理サービス提供者 71 は顧客ネットワーク 72 からシステム情報（顧客ネットワークの情報）10A を取得し、フィルタリングルール及びパッチ 30 が必要なシステム情報 10B だけを情報サービス提供者 70 に送信する。情報サービス提供者 70 は、独自のセキュリティ情報を用いて顧客ネットワーク 72 毎にパッチおよびフィルタリングルール 30 を作成し、管理サービス提供者 71 に送信し、当該管理サービス提供者 71 が顧客ネットワーク 72 に当該パッチおよびフィルタリングルールを提供する。

【0073】

実施の形態 9.

図 20 は本発明の実施の形態 9 として、各システムの第 3 の配属構成を示している。

図 20 に示す例では、情報サービス提供者 70 はセキュリティ情報 30A を送信するだけで、管理サービス提供者 71 が予防システム 4 および回復システム 5 を有する。管理サービス提供者 71 は情報サービス提供者 70 からセキュリティ情報 30A をダウンロードし、顧客ネットワーク 72 からシステム情報（顧客ネットワークの情報）10A を取得し、顧客ネットワーク 72 毎にパッチおよびフィルタリングルール 30 を作成し、顧客ネットワーク 72 に当該パッチおよびフィルタリングルール 30 を提供する。

【0074】

実施の形態 10.

図 21 は本発明の実施の形態 10 として、各システムの第 4 の配属構成を示し

ている。

図 21 に示す例では、1 つの管理サービス提供者 71 が 4 つの情報サービス提供者 70 からセキュリティ情報 I 2 を取得し、被害を受けた顧客ネットワーク A の回復を行う。更に、当該管理サービス提供者 71 が当該顧客ネットワーク A から被害に関する情報 I 1 を取得し、当該情報 I 1 を元にその他 3 つの顧客ネットワーク 1 (B ~ D) の予防に役立てる (被害情報、対策情報をフィードバックすることができる)。また、当該被害に関する情報を 4 つの情報サービス提供者 70 (A ~ D) に送信する。

【0075】

以上に詳述したように、本発明の実施の形態によれば、予防システム、回復システムおよび情報提供装置が連携することにより、万が一被害を受けても被害範囲の同定を容易に行うことができる。また、回復システム (診断部) により被害隔離および修復が行われ、被害を最小限に抑えると共に、所定の被害については自動的に且つ迅速に修復することが可能となる。またそこで得た被害に関する情報を蓄積し再利用することができるので、同じ被害が異なる場所で生じないようにすることもできる。さらに、単にパッチ適用を行うだけでなく、その後パッチを適用した対象マシンに対して動作確認を自動で行い、パッチ適用を行ったマシンの動作がパッチ適用前と変わっていないことをも検証でき、セキュリティ対策として極めて役立ち得るものである。更に、顧客ネットワークに対し、数多くの情報サービス提供者が提供する情報を整理して提供することができ、顧客側にとっては、情報処理の煩雑さが軽減される。

【0076】

(付記 1) ネットワークにおけるセキュリティに関する情報を提供するセキュリティ情報提供部から取得されるセキュリティ情報と、ネットワークに接続された少なくとも一つのネットワークマシンから取得されるマシン情報とに基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、セキュリティ関連処理の種別とその必要性の有無を判断するセキュリティ診断部と、

前記セキュリティ診断部による診断結果に基づいて、前記ネットワークマシン

若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、所定のセキュリティ対策処理を行うセキュリティ実行部とを備えてなるセキュリティ管理装置。

(付記2) 付記1に記載のセキュリティ管理装置において、

前記セキュリティ診断部は、さらに、前記ネットワークに接続され、又は前記ネットワークに接続される可能性のあるネットワークマシンについての所定の情報を記憶したマシン関連情報記憶部から得られるマシン関連情報に基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、セキュリティ関連処理の種別とその必要性の有無を判断することを特徴とするセキュリティ管理装置。

(付記3) 付記2に記載のセキュリティ管理装置において、

前記マシン関連情報記憶部に記憶されたマシン関連情報は、セキュリティポリシーについて規定した情報であることを特徴とするセキュリティ管理装置。

(付記4) 付記3に記載のセキュリティ管理装置において、

前記セキュリティポリシーは、所定のマシン情報についてのフィルタリング防御又は通信制御について規定し、前記セキュリティ実行部はフィルタリング処理又は通信制御を実行することを特徴とするセキュリティ管理装置。

(付記5) 付記3に記載のセキュリティ管理装置において、

前記セキュリティポリシーは、所定のプログラムについてのパッチ適用又はワクチン投与について規定し、前記セキュリティ実行部は前記所定のプログラムにパッチ適用処理又はワクチン投与処理を実行することを特徴とするセキュリティ管理装置。

(付記6) 付記5に記載のセキュリティ管理装置において、

前記セキュリティ実行部によるセキュリティ対策処理が実行された場合に、その実行結果における前記ネットワークマシン若しくはネットワークにおける動作確認が行われることを特徴とするセキュリティ管理装置。

(付記7) 付記5に記載のセキュリティ管理装置において、

前記セキュリティ実行部によるセキュリティ対策処理が実行された場合において、そのセキュリティ対象についてフィルタリングルールが設定されている場合

は、そのルールの削除が行われることを特徴とするセキュリティ管理装置。

(付記 8) 付記 1 又は付記 2 に記載のセキュリティ管理装置において、

さらに新規に導入されるネットワークマシンからの接続要求を受け付ける接続要求受付部を備え、前記セキュリティ診断部は、前記接続要求受付部により新規ネットワークマシンからの接続要求を受け付けた場合に、前記マシンを離隔状態として該ネットワークマシンにアドレスを与え、前記マシン情報と前記セキュリティ情報とに基づいて、前記セキュリティ関連処理として前記ネットワークマシンに対する離隔解除を行うか否かを判断することを特徴とするセキュリティ管理装置。

(付記 9) 付記 1 又は付記 2 に記載のセキュリティ管理装置において、

さらに新規に導入されるネットワークマシンからの接続要求を受け付ける接続要求受付部を備え、前記セキュリティ診断部は、前記接続要求受付部により新規ネットワークマシンからの接続要求を受け付けると共に、前記ネットワークマシンからマシン情報を受け付けると、該マシン情報と前記セキュリティ情報とに基づいて、前記セキュリティ関連処理として前記ネットワークマシンに対するアドレス付与の可否を判断することを特徴とするセキュリティ管理装置。

(付記 10) ネットワークに接続された少なくとも一つのネットワークマシンから取得されるマシン情報と、前記ネットワークに接続され、又は前記ネットワークに接続される可能性のあるネットワークマシンについての所定の情報を記憶したマシン関連情報記憶部から得られるマシン関連情報とに基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、セキュリティ関連処理の種別とその必要性の有無を判断するセキュリティ診断部と、

前記セキュリティ診断部による診断結果に基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、所定のセキュリティ対策処理を行うためのセキュリティ実行部とを備えてなるセキュリティ管理装置。

(付記 11) 付記 10 に記載のセキュリティ管理装置において、

前記マシン関連情報は、コンピュータウィルスの挙動内容を示す情報を含み、

前記マシン情報には所定のファイルのハッシュ値、ウィルススキャン結果の少なくともいずれか一つを含み、

前記セキュリティ診断部は、所定のネットワークマシンについて、離隔する必要性の有無を判断し、前記セキュリティ実行部は前記セキュリティ診断部により前記ネットワークマシンを離隔する必要があると判断された場合には、前記ネットワークマシンを離隔するための処理を行うことを特徴とするセキュリティ管理装置。

(付記 12) 付記 10 に記載のセキュリティ管理装置において、

前記ネットワークマシンの通信を監視するネットワーク監視部を備え、

前記マシン関連情報は、ネットワークマシンのプロファイルに関する情報であり、

前記セキュリティ診断部は、前記ネットワーク監視部からの監視情報と前記マシン情報と前記ネットワークマシンのプロファイルに関する情報とに基づいて、所定のネットワークマシンについて、離隔する必要性の有無を判断し、

前記セキュリティ実行部は前記セキュリティ診断部により前記ネットワークマシンを離隔する必要があると判断した場合には、前記ネットワークマシンを離隔するための処理を行うことを特徴とするセキュリティ管理装置。

(付記 13) 付記 10 乃至付記 12 のいずれかに記載のセキュリティ管理装置において、

前記セキュリティ診断部は、被害範囲の同定を行い、離隔範囲を定めることを特徴とするセキュリティ管理装置。

(付記 14) 付記 10 乃至付記 13 のいずれかに記載のセキュリティ管理装置において、

前記セキュリティ診断部の診断結果に基づき、所定の被害を受けたネットワークマシン若しくはネットワークに対して修復を行うための修復部が備えられていることを特徴とするセキュリティ管理装置。

(付記 15) 付記 10 乃至付記 14 のいずれかに記載のセキュリティ管理装置において、

被害修復が行われた場合、離隔を解除する離隔解除部が備えられていることを

特徴とするセキュリティ管理装置。

(付記 16) 付記 10 に記載のセキュリティ管理装置において、

前記マシン情報は、機器構成の変更の通知と、少なくともその変更される機器構成の情報を含み、前記マシン関連情報は、前記ネットワークにおいて使用の可否を規定した機器構成情報を含むことを特徴とするセキュリティ管理装置。

(付記 17) 付記 16 に記載のセキュリティ管理装置において、

前記セキュリティ診断部は、前記ネットワークマシンの離隔の必要性について判断し、セキュリティ実行部は前記セキュリティ診断部の判断結果に基づいて前記ネットワークマシンを離隔するための処理を行うことを特徴とするセキュリティ管理装置。

(付記 18) ネットワークにおけるセキュリティに関するセキュリティ情報を提供するセキュリティ情報提供装置と、

前記ネットワークに接続され、又は前記ネットワークに接続される可能性のあるネットワークマシンについての所定の情報を記憶したマシン関連情報データベースと、

前記セキュリティ情報提供部から得られるセキュリティ情報と、前記マシン関連情報データベースから得られるマシン関連情報と、ネットワークに接続された少なくとも一つのネットワークマシンから取得されるマシン情報とに基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、被害の有無の判断、または予防の必要性の有無の判断を行う予防システムと、

前記予防システムの判断に基づいて、所定の被害がある場合には修復処理を行い、または予防措置をとる回復システムと

を備えてなるセキュリティ管理システム。

(付記 19) 付記 18 に記載のセキュリティ管理システムにおいて、

前記予防システム又は前記回復システムは複数設けられ、これらシステムを統括的に管理する管理センタが設けられていることを特徴とするセキュリティ管理システム。

(付記 20) 付記 18 に記載のセキュリティ管理システムにおいて、

前記予防システム又は前記回復システムは複数設けられ、これら複数のシステムのそれぞれで取得された情報が互いに共有されることを特徴とするセキュリティ管理システム。

(付記 2 1) 付記 1 8 乃至付記 2 0 のいずれかに記載のセキュリティ管理システムにおいて、

前記セキュリティ情報提供部の所有者側に前記予防システム及び前記回復システムが設けられていることを特徴とするセキュリティ管理システム。

(付記 2 2) 付記 1 8 乃至付記 2 0 のいずれかに記載のセキュリティ管理システムにおいて、

前記セキュリティ情報提供部の所有者側に前記予防システムが設けられ、管理サービスを提供する管理サービス提供者側に前記回復システムが設けられることを特徴とするセキュリティ管理システム。

(付記 2 3) 付記 1 8 乃至付記 2 0 のいずれかに記載のセキュリティ管理システムにおいて、

管理サービスを提供する管理サービス提供者側に前記予防システム及び前記回復システムが設けられることを特徴とするセキュリティ管理システム。

(付記 2 4) 付記 1 8 乃至付記 2 3 のいずれかに記載のセキュリティ管理システムにおいて、

前記回復システムにおいて取得された所定の情報が新たなセキュリティ情報として、前記予防システムにフィードバックされることを特徴とするセキュリティ管理システム。

(付記 2 5) ネットワークにおけるセキュリティに関するセキュリティ情報を取得するセキュリティ情報取得ステップと、

ネットワークに接続された少なくとも一つのネットワークマシンからマシン情報を取得するマシン情報取得ステップと、

前記セキュリティ情報及び前記マシン情報とに基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、セキュリティ関連処理の種別とその必要性の有無を判断するセキュリティ診断ステップと、

前記セキュリティ診断ステップによる診断結果に基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、所定のセキュリティ対策処理を行うセキュリティ実行ステップと

を備えてなるセキュリティ管理方法。

(付記 26) 付記 25 に記載のセキュリティ管理方法において、

さらに、前記ネットワークに接続され、又は前記ネットワークに接続される可能性のあるネットワークマシンについての所定の情報を記憶したマシン関連情報記憶部から得られるマシン関連情報を取得するマシン関連情報取得ステップを備え、

前記セキュリティ診断ステップでは、前記セキュリティ情報及び前記マシン情報とともに、前記マシン関連情報に基づいて、前記セキュリティ診断を行うことを特徴とするセキュリティ管理方法。

(付記 27) ネットワークに接続された少なくとも一つのネットワークマシンからマシン情報を取得するマシン情報取得ステップと、

前記ネットワークに接続され、又は前記ネットワークに接続される可能性のあるネットワークマシンについての所定の情報を記憶したマシン関連情報記憶部からマシン関連情報を取得するマシン関連情報取得ステップと、

前記マシン情報とマシン関連情報とに基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、セキュリティ関連処理の種別とその必要性の有無を判断するセキュリティ診断ステップと

前記セキュリティ診断部による診断結果に基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、所定のセキュリティ対策処理を行うためのセキュリティ実行ステップと

を備えてなるセキュリティ管理方法。

(付記 28) セキュリティ管理をコンピュータに実行させるセキュリティ管理プログラムであって、

ネットワークにおけるセキュリティに関するセキュリティ情報を取得するセキュリティ情報取得ステップと、

ネットワークに接続された少なくとも一つのネットワークマシンからマシン情報を取得するマシン情報取得ステップと、

前記セキュリティ情報及び前記マシン情報とに基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、セキュリティ関連処理の種別とその必要性の有無を判断するセキュリティ診断ステップと、

前記セキュリティ診断ステップによる診断結果に基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、所定のセキュリティ対策処理を行うセキュリティ実行ステップと

をコンピュータに実行させるセキュリティ管理プログラム。

(付記 29) 付記 28 に記載のセキュリティ管理プログラムにおいて、

さらに、前記ネットワークに接続され、又は前記ネットワークに接続される可能性のあるネットワークマシンについての所定の情報を記憶したマシン関連情報記憶部から得られるマシン関連情報を取得するマシン関連情報取得ステップを備え、

前記セキュリティ診断ステップでは、前記セキュリティ情報及び前記マシン情報とともに、前記マシン関連情報に基づいて、前記セキュリティ診断を行うことをコンピュータに実行させるセキュリティ管理プログラム。

(付記 30) セキュリティ管理をコンピュータに実行させるセキュリティ管理プログラムであって、

ネットワークに接続された少なくとも一つのネットワークマシンからマシン情報を取得するマシン情報取得ステップと、

前記ネットワークに接続され、又は前記ネットワークに接続される可能性のあるネットワークマシンについての所定の情報を記憶したマシン関連情報記憶部からマシン関連情報を取得するマシン関連情報取得ステップと、

前記マシン情報とマシン関連情報とに基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、セキュリティ関連処理の種別とその必要性の有無を判断するセキュリティ診断ステップと、

前記セキュリティ診断部による診断結果に基づいて、前記ネットワークマシン若しくは前記ネットワークマシンが含まれる所定のネットワークに対して、所定のセキュリティ対策処理を行うためのセキュリティ実行ステップと
をコンピュータに実行させるセキュリティ管理プログラム。

【0077】

【発明の効果】

以上に詳述したように、本発明によれば、ネットワークを構成するネットワークマシンからマシン情報を取得し、このマシン情報を参照しつつ種々のセキュリティ対策を講じることができ、もって柔軟性に優れ、幅広く適用することが可能なセキュリティ管理装置、セキュリティ管理システム、セキュリティ管理方法、セキュリティ管理プログラムを提供することができるという効果を奏する。

【図面の簡単な説明】

【図1】

本発明の実施の形態におけるセキュリティ管理システムの全体構成を原理的に示すブロック図である。

【図2】

本発明の実施の形態の全体構成を示すブロック図である。

【図3】

本発明の実施の形態1を示すブロック図である。

【図4】

セキュリティ管理が実施されるネットワークを示すブロック図である。

【図5】

実施の形態1の動作を示すフローチャートである。

【図6】

本発明の実施の形態2を示すブロック図である。

【図7】

本発明の実施の形態2の動作を示すフローチャートである。

【図8】

本発明の実施の形態3を示すブロック図である。

【図 9】

本発明の実施の形態 3 において、被害の有無を判断する動作を示す概念図である。

【図 10】

本発明の実施の形態 3 の動作を示すフローチャートである。

【図 11】

実施の形態 4 を示すブロック図である。

【図 12】

本発明の実施の形態 4 の動作を示すフローチャートである。

【図 13】

本発明の実施の形態 5 を示すブロック図である。

【図 14】

本発明の実施の形態 5 の動作を示すフローチャートである。

【図 15】

本発明の実施の形態 6 を示すブロック図である。

【図 16】

本発明の実施の形態 6 の動作を示すフローチャートである。

【図 17】

本発明の実施の形態におけるマシン情報の一例を示す図である。

【図 18】

本発明の実施の形態 7 として、各システムの第 1 の配属構成を示す図である。

【図 19】

本発明の実施の形態 8 として、各システムの第 2 の配属構成を示す図である。

【図 20】

本発明の実施の形態 9 として、各システムの第 3 の配属構成を示す図である。

【図 21】

本発明の実施の形態 10 として、各システムの第 4 の配属構成を示す図である。

。

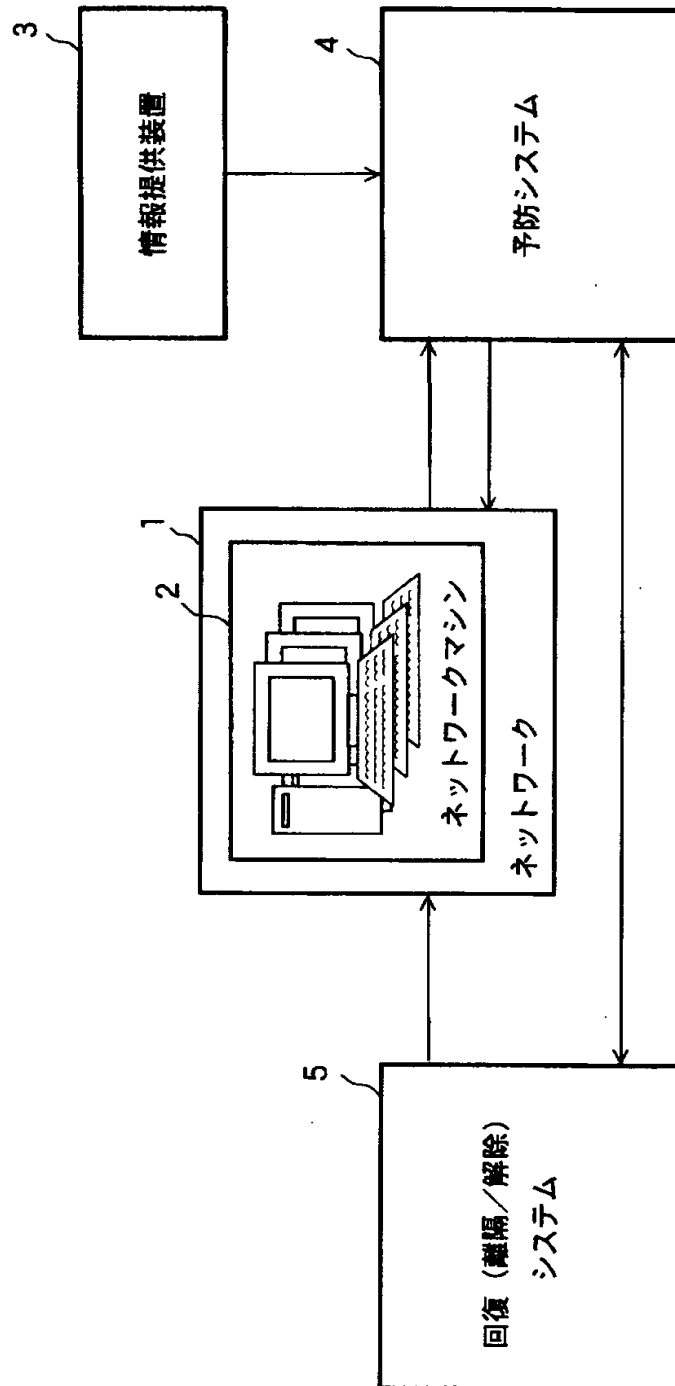
【符号の説明】

1 ネットワーク、2 ネットワークマシン、3 情報提供装置、4 予防システム、5 回復システム、4 1 診断部、4 2 各種データベース、4 3 ネットワーク監視装置、4 4 予防実行部、7 0 情報サービス提供者、7 1 管理サービス提供者、7 2 顧客ネットワーク、4 1 1 情報取得部、4 1 2 情報検索／比較部、4 1 3 判定部。

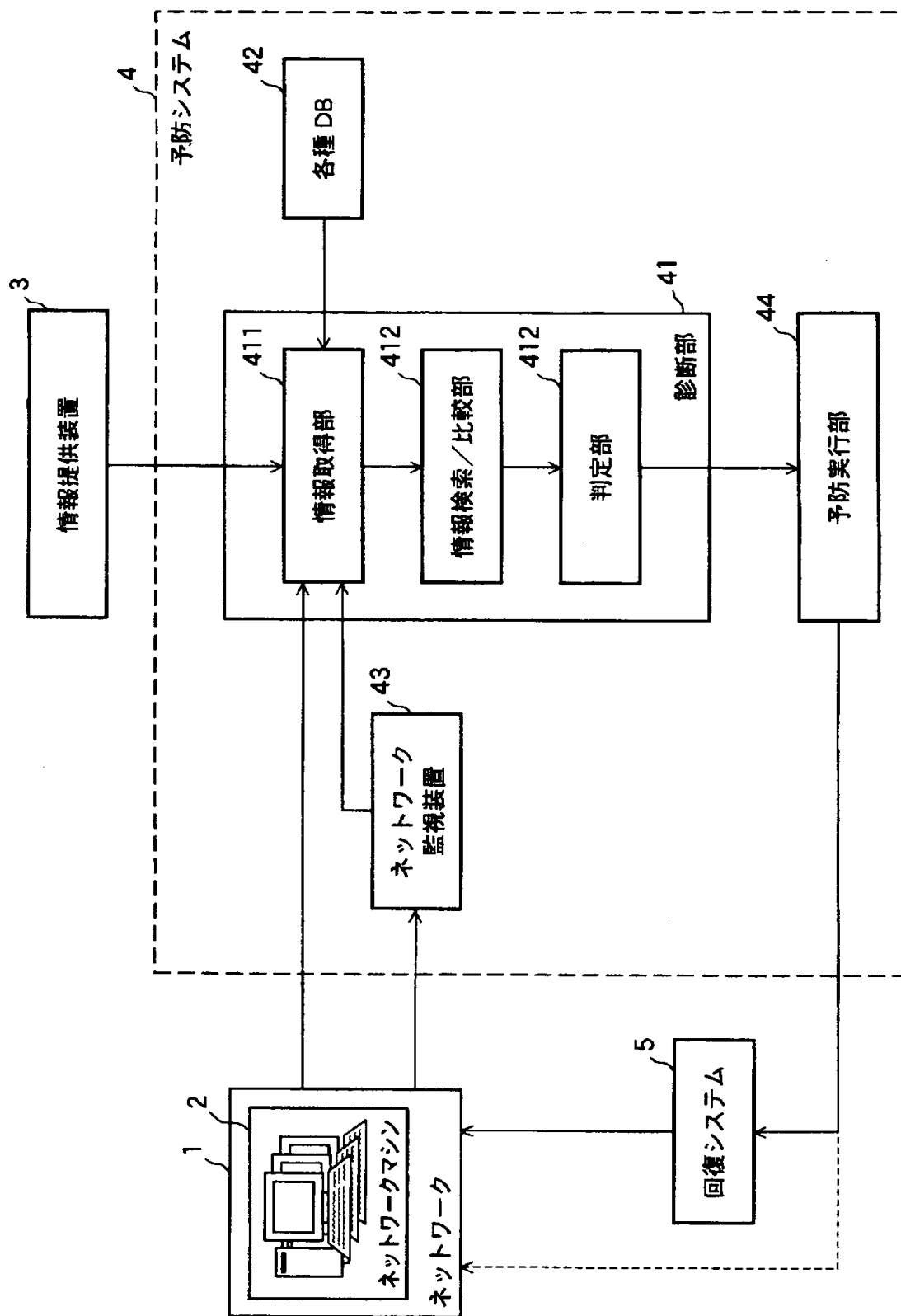
【書類名】

図面

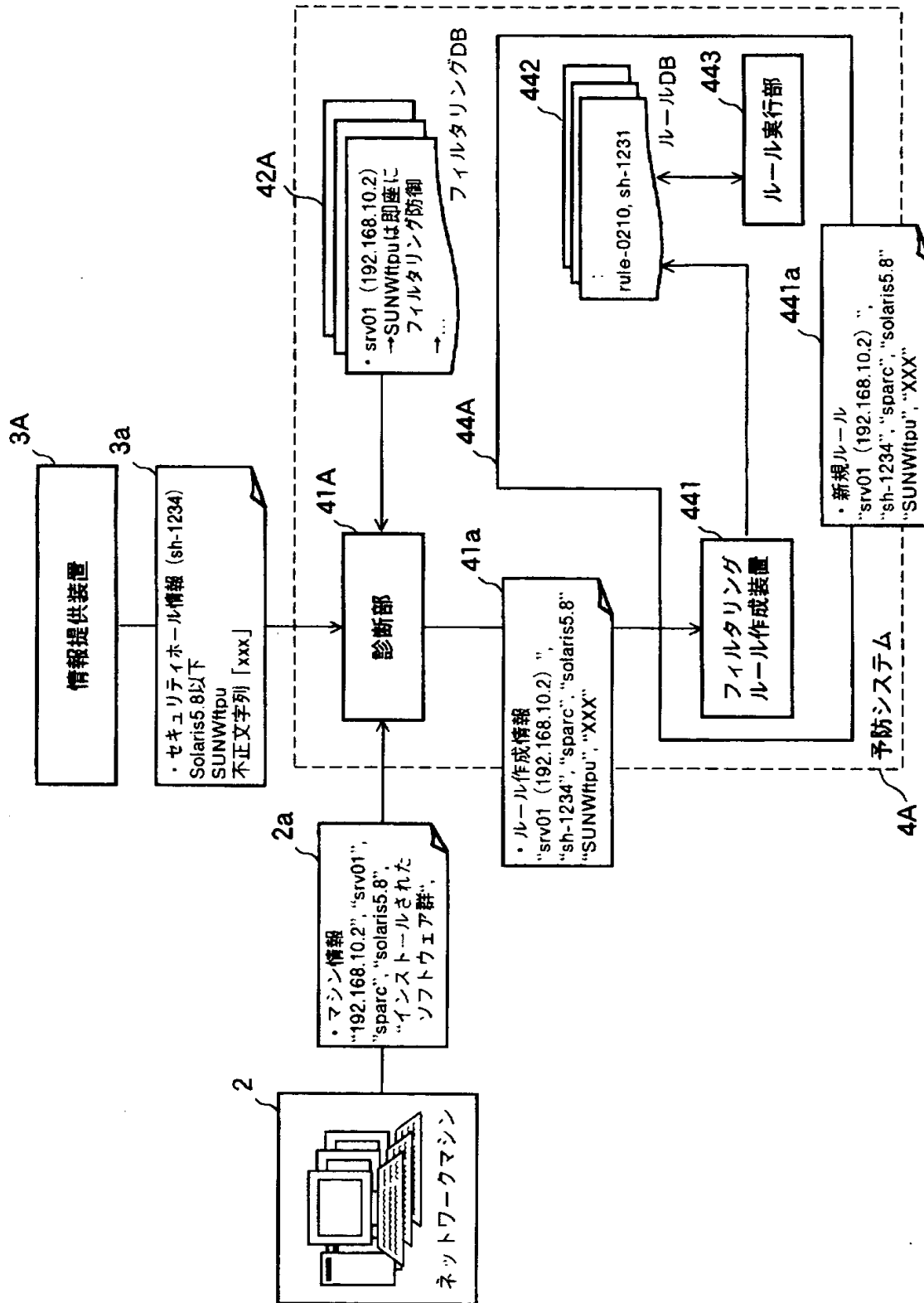
【図 1】



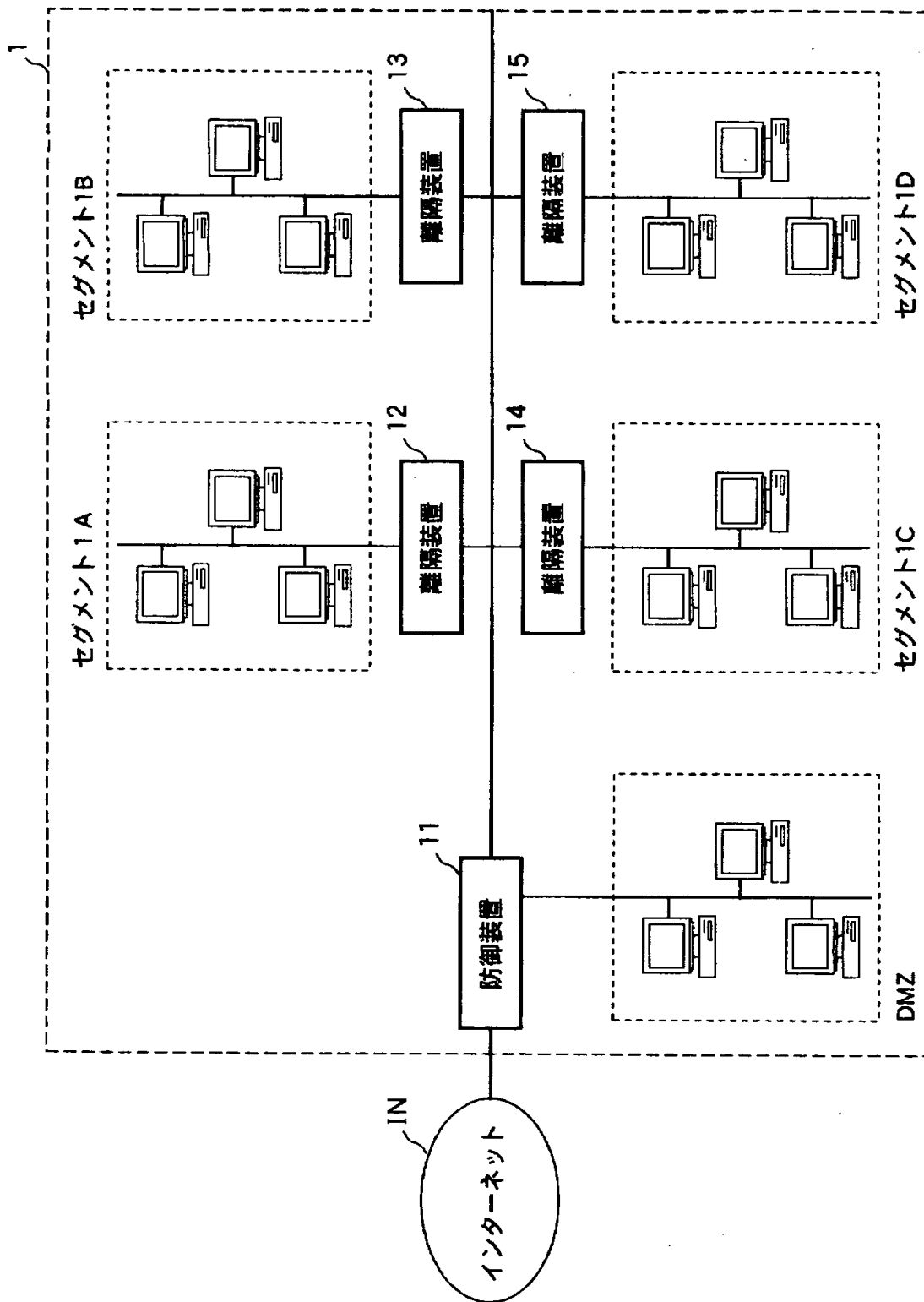
【図 2】



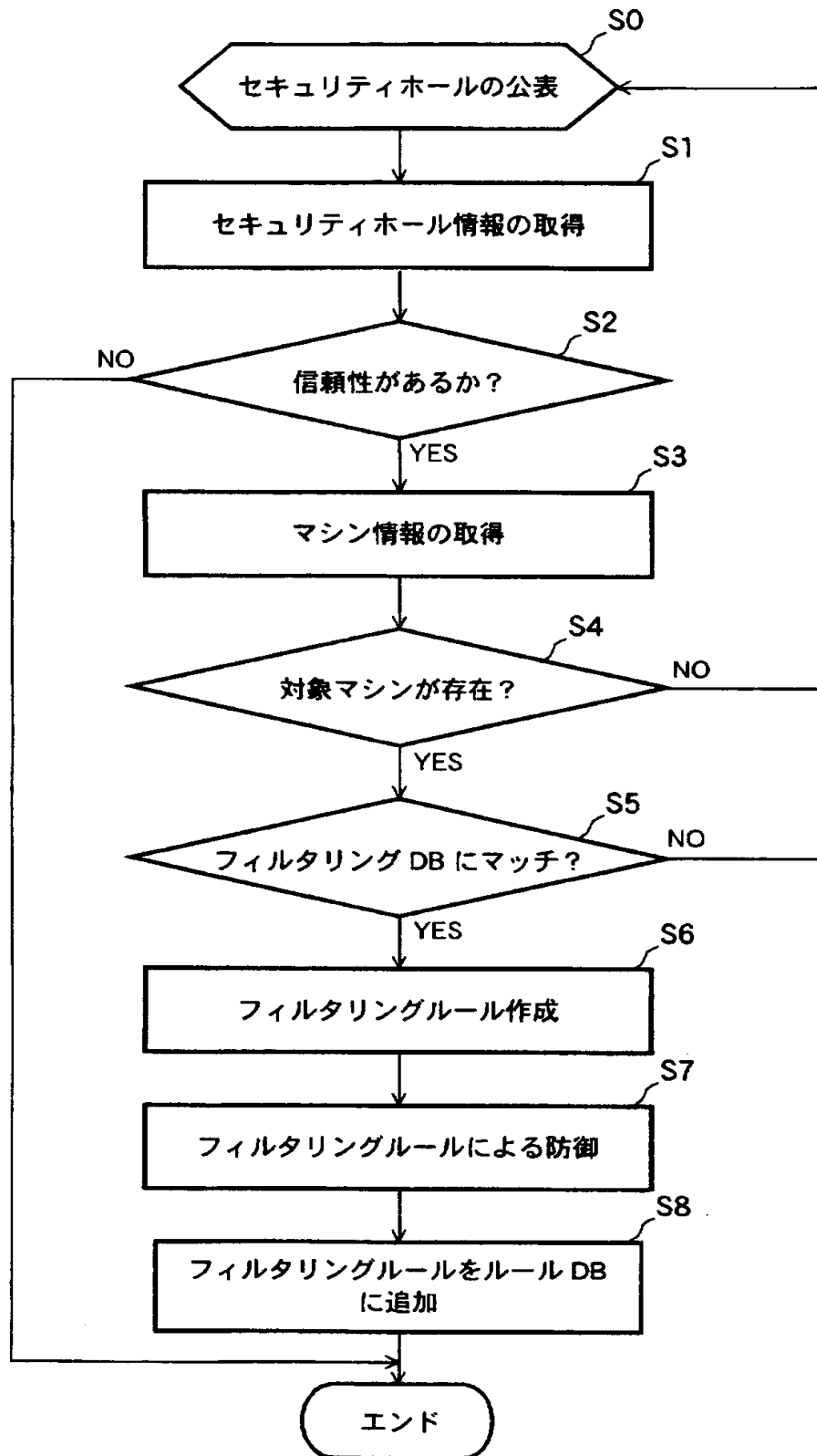
【図3】



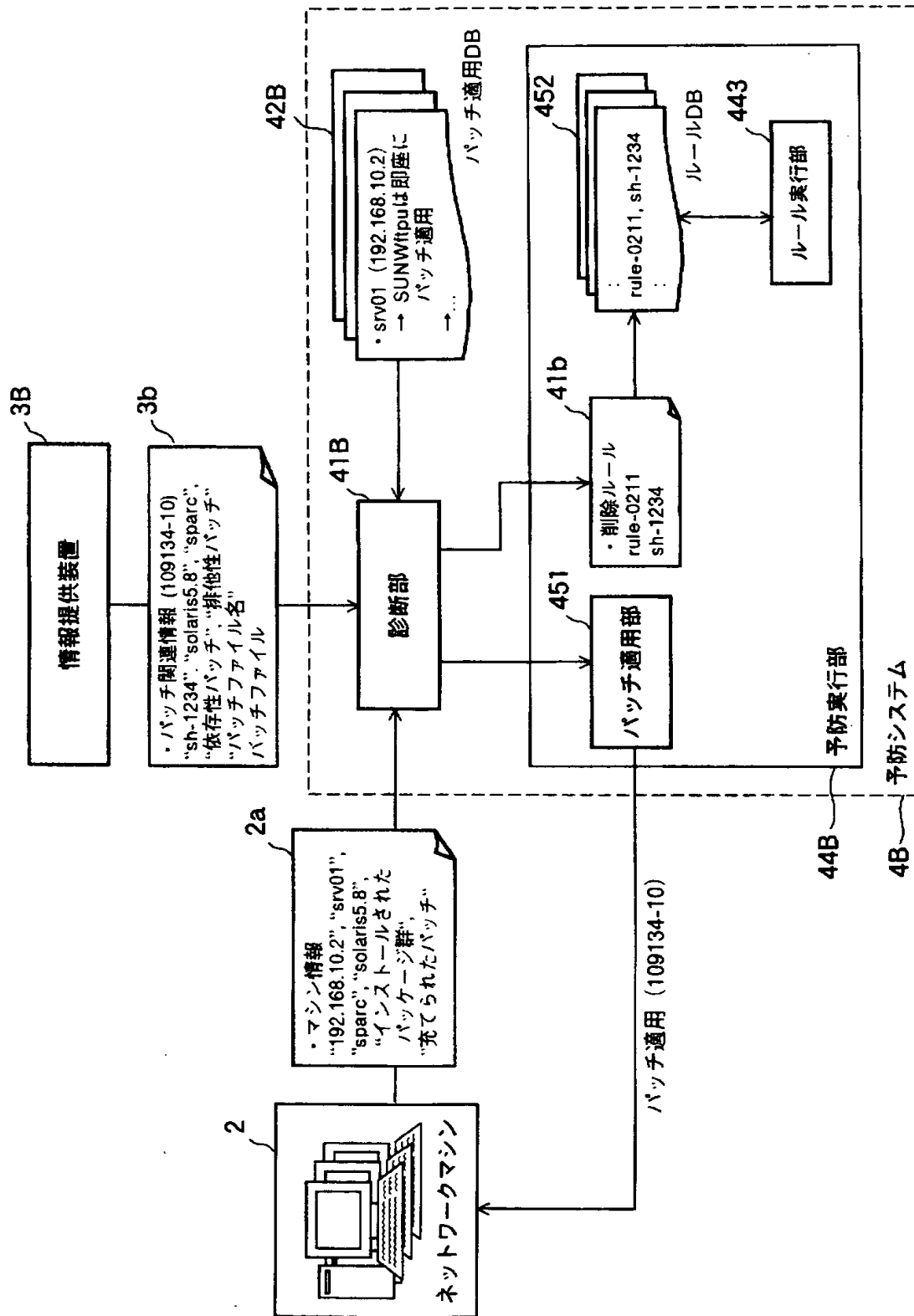
【図 4】



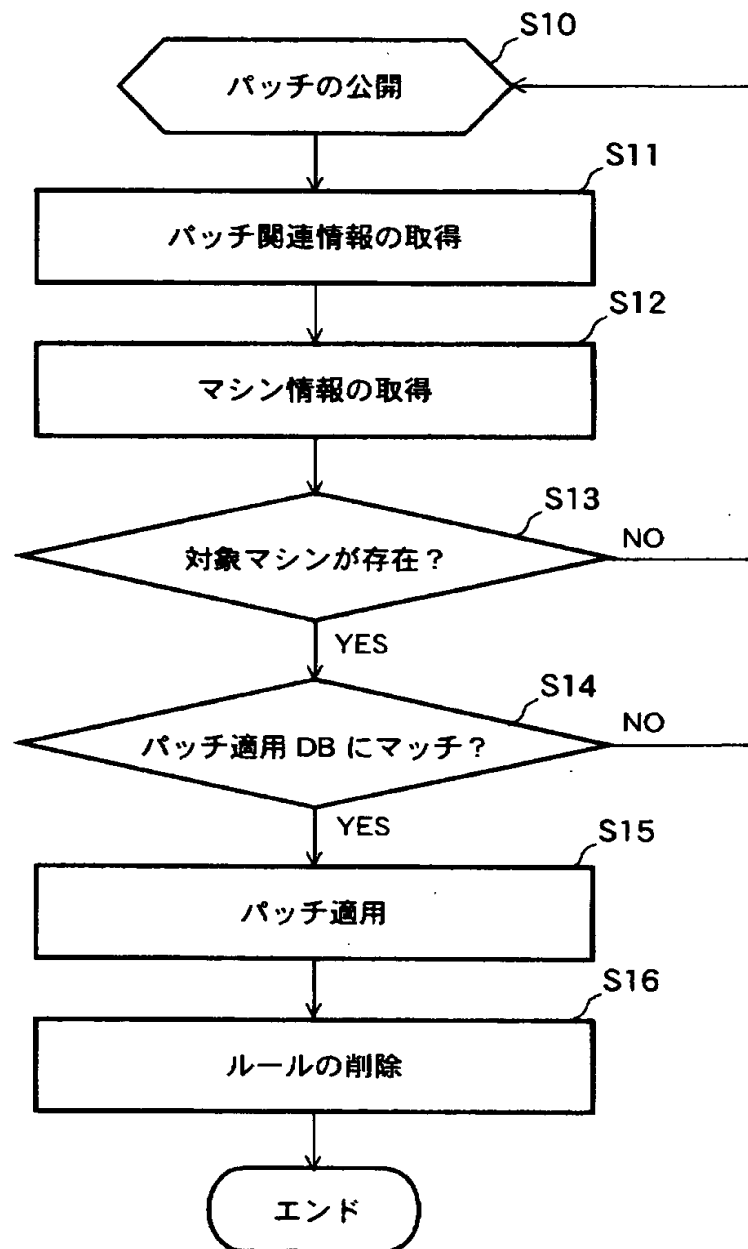
【図 5】



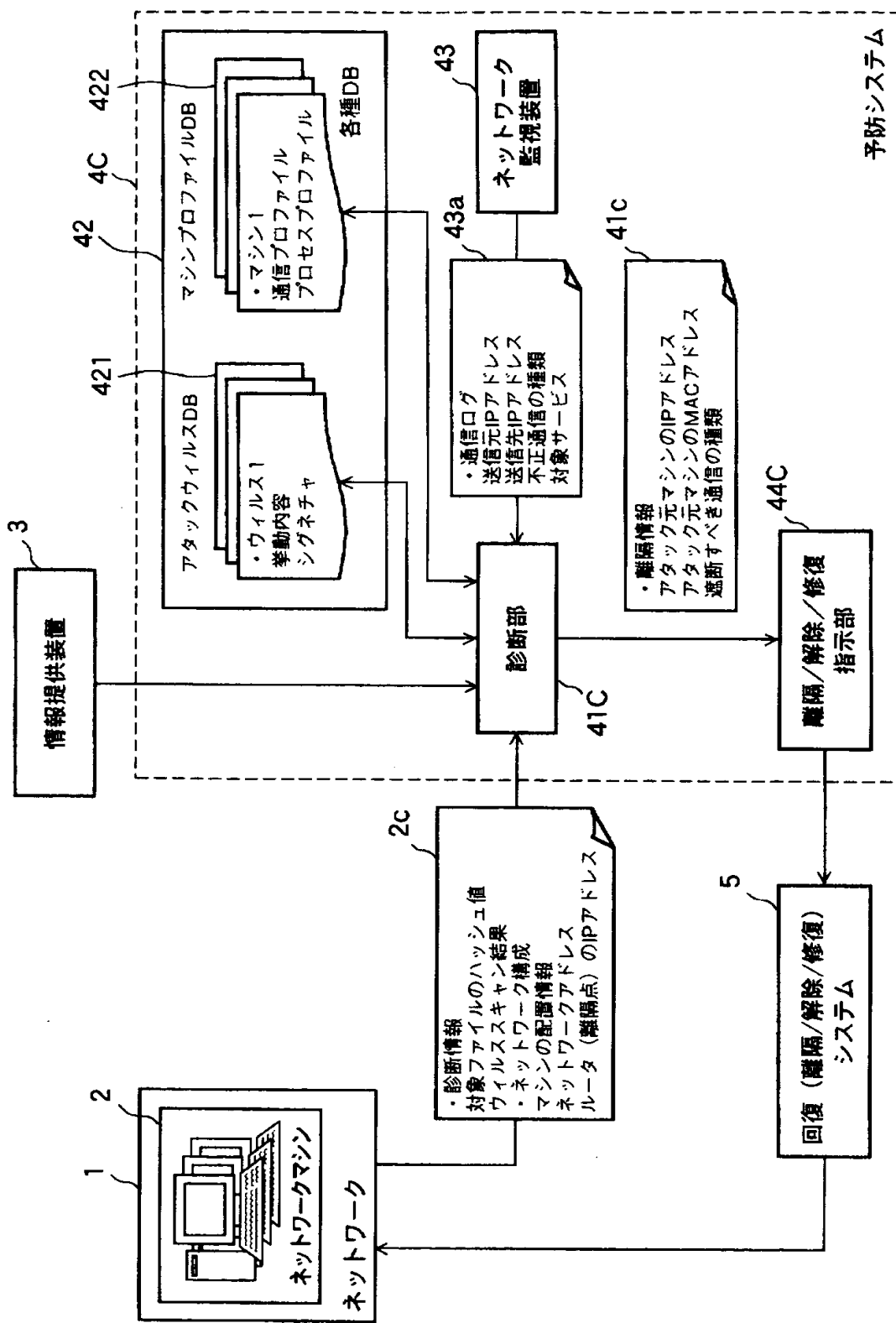
【図 6】



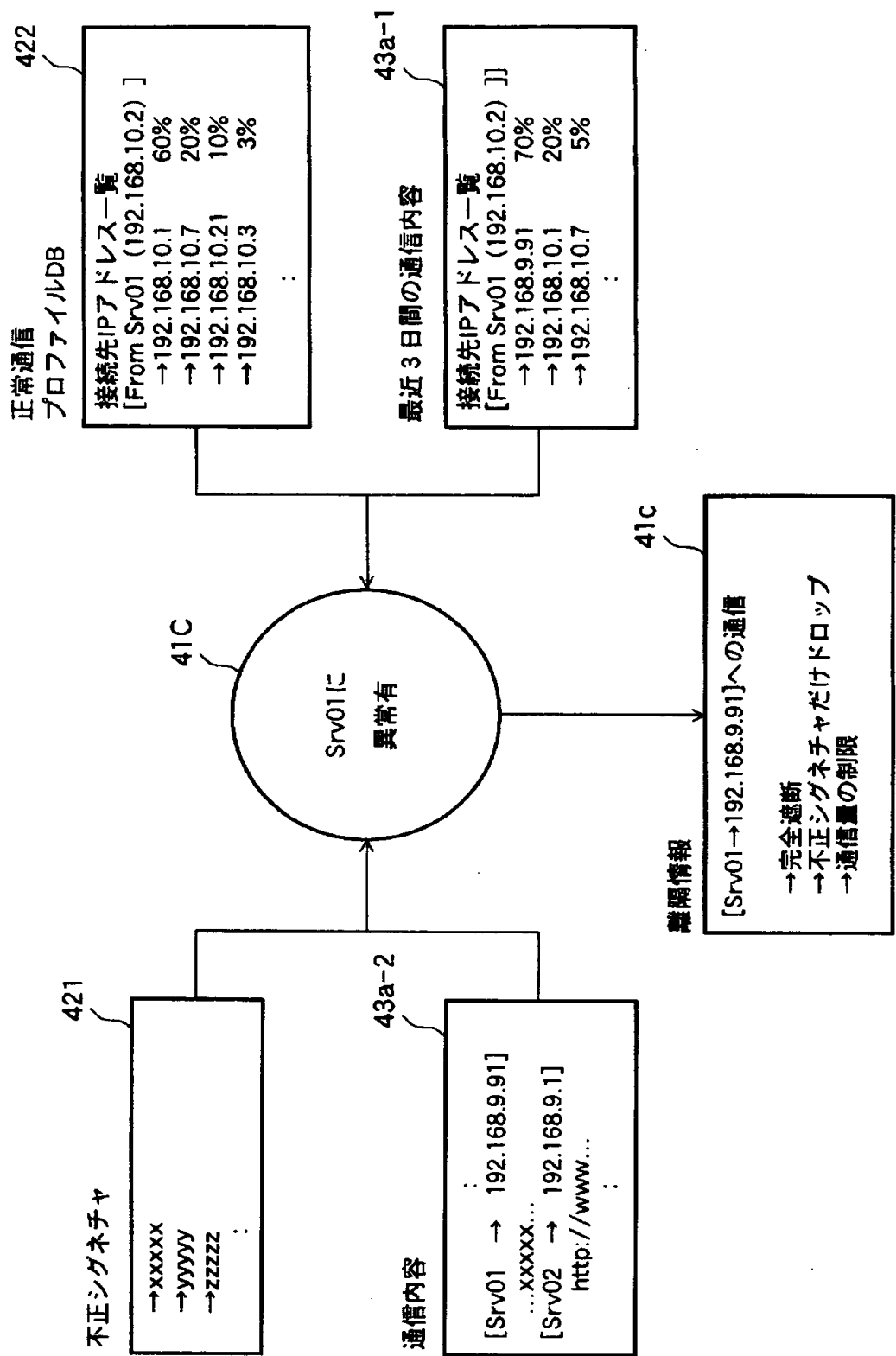
【図 7】



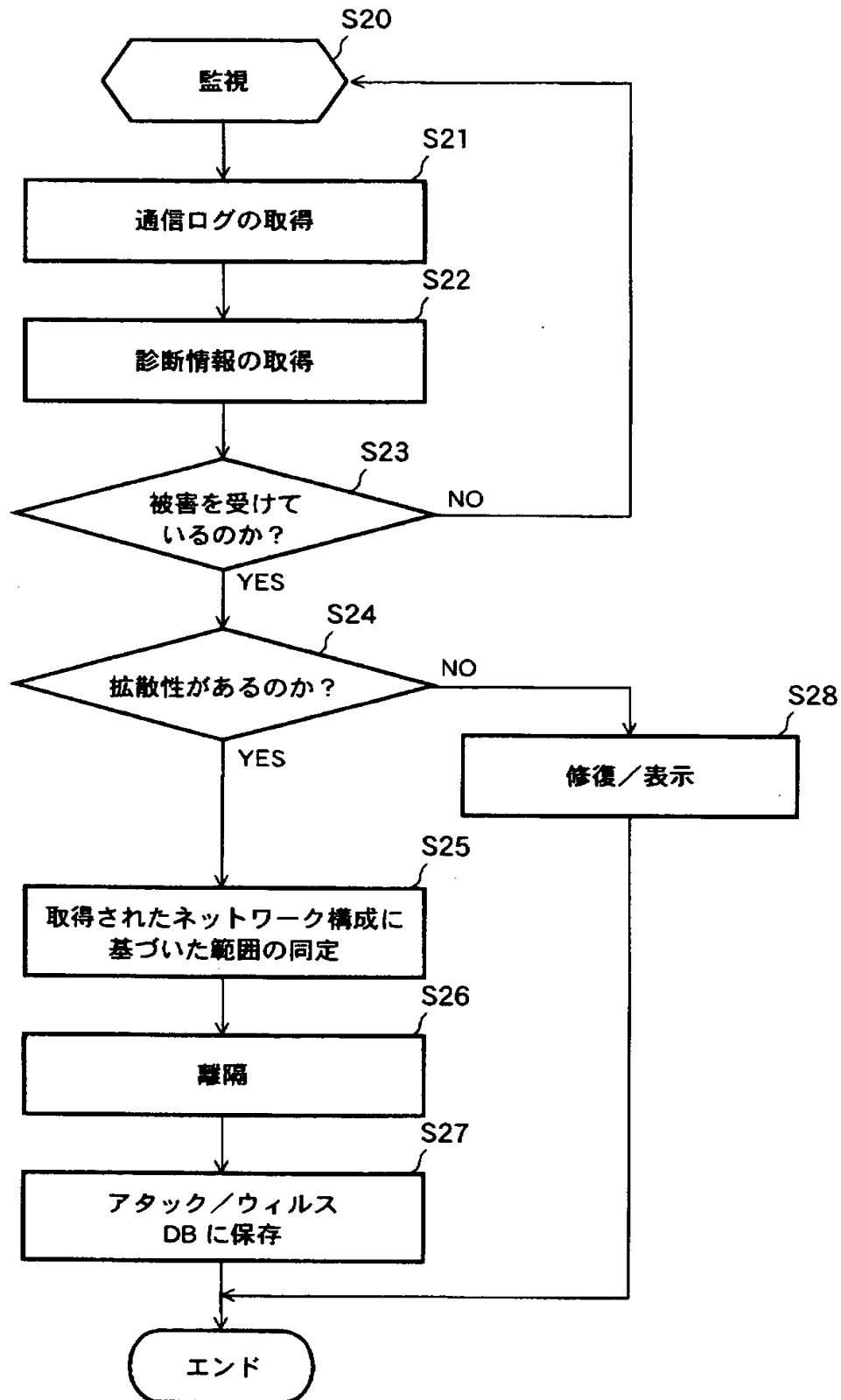
【図 8】



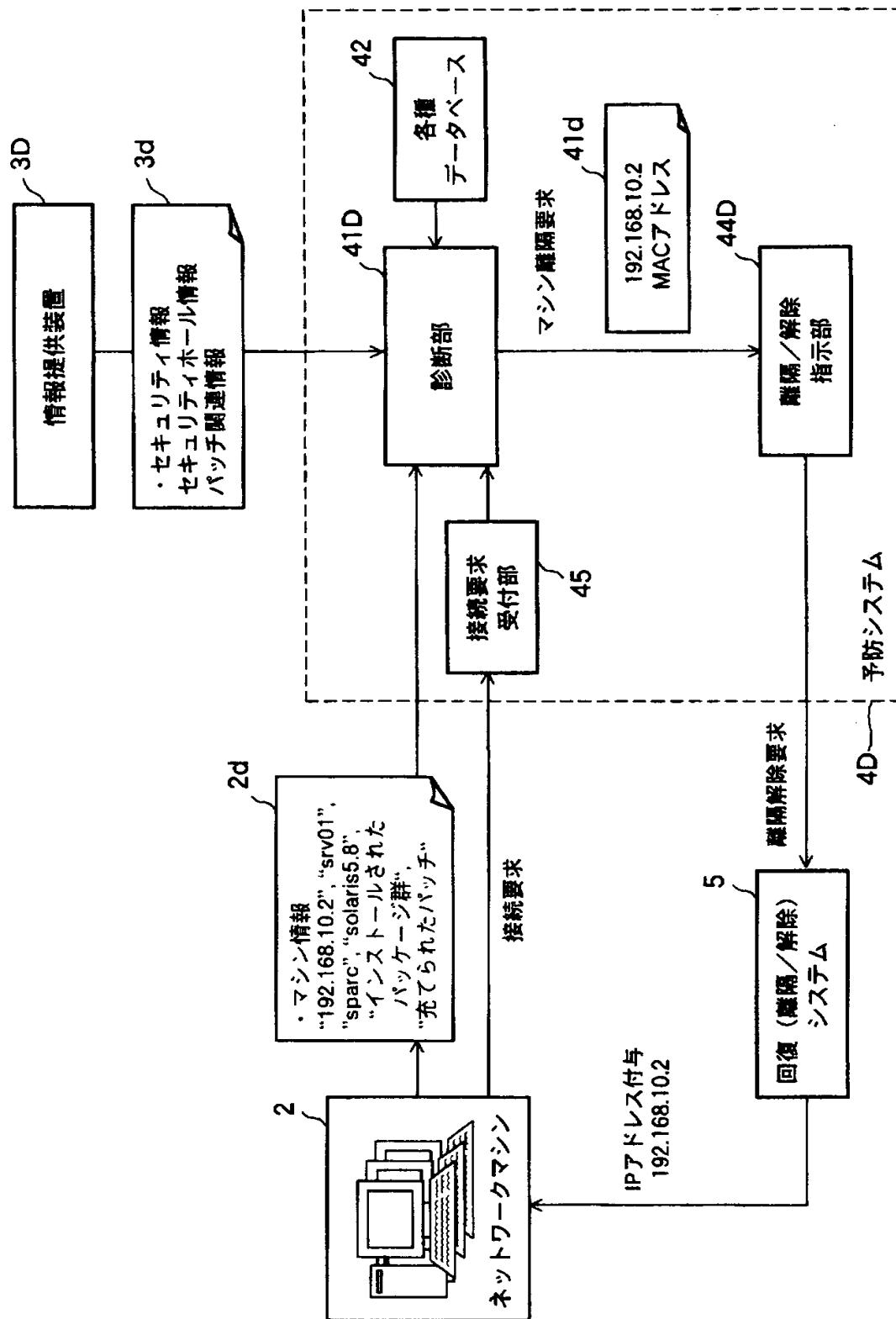
【図9】



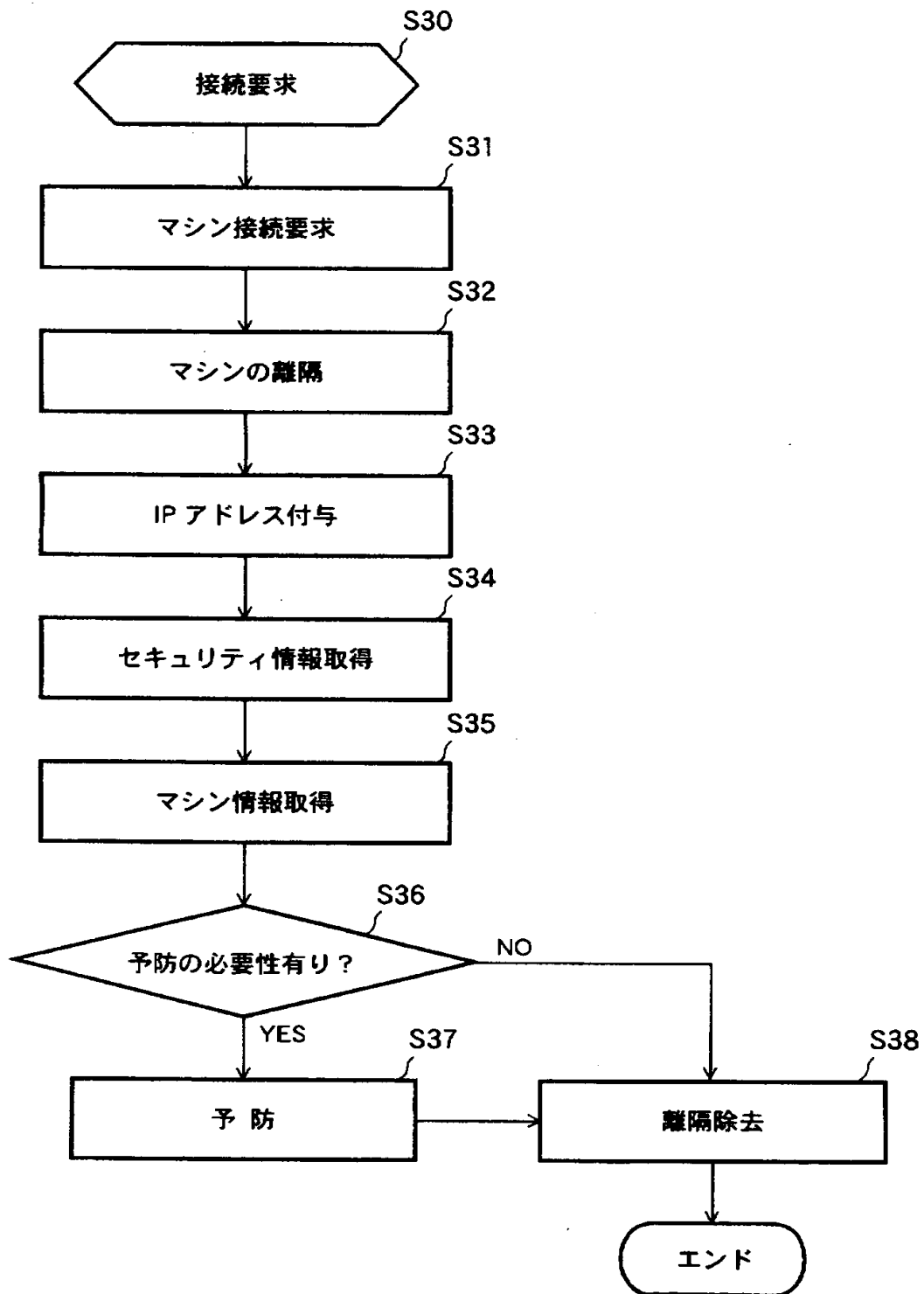
【図 10】



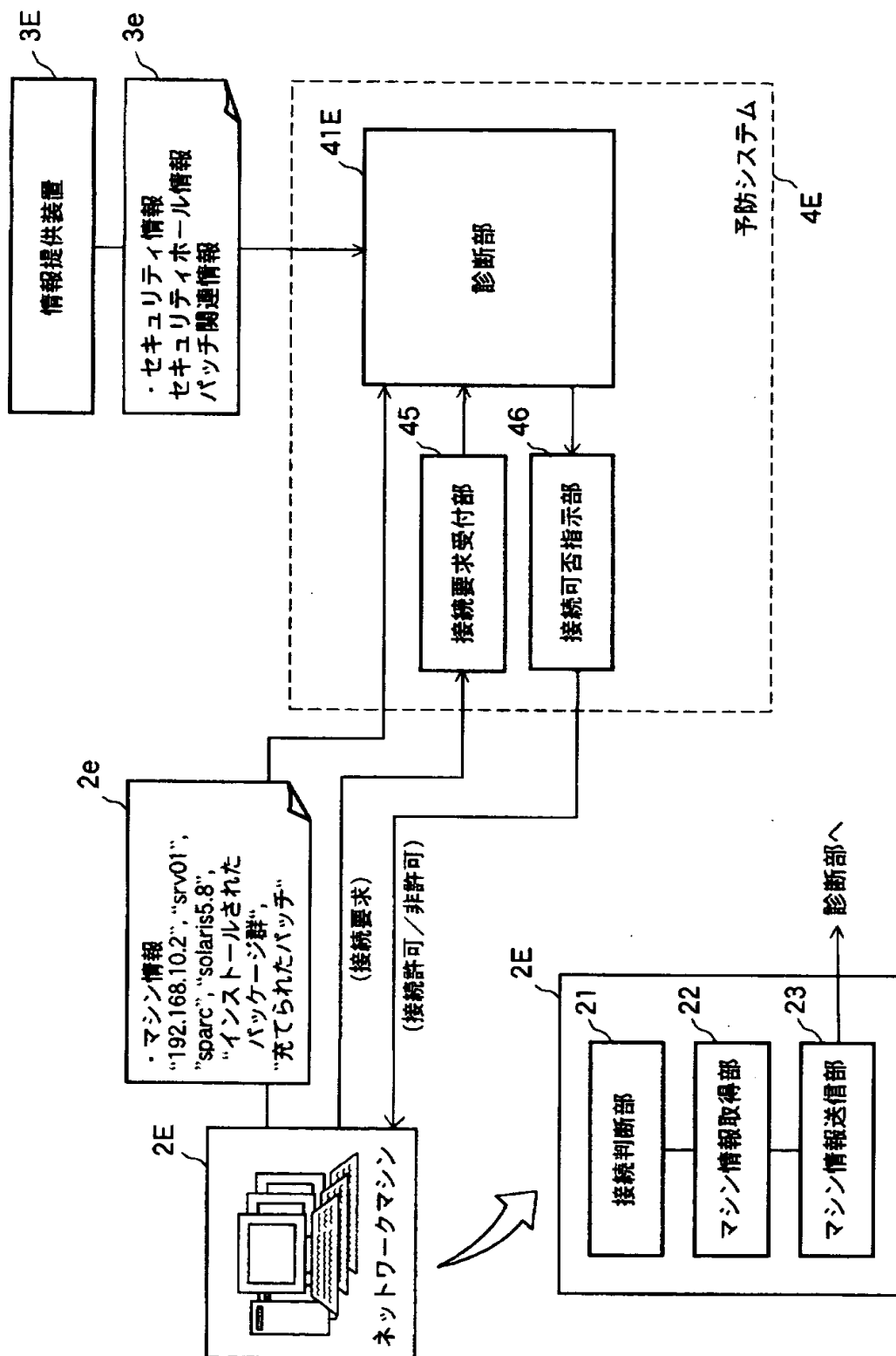
【図11】



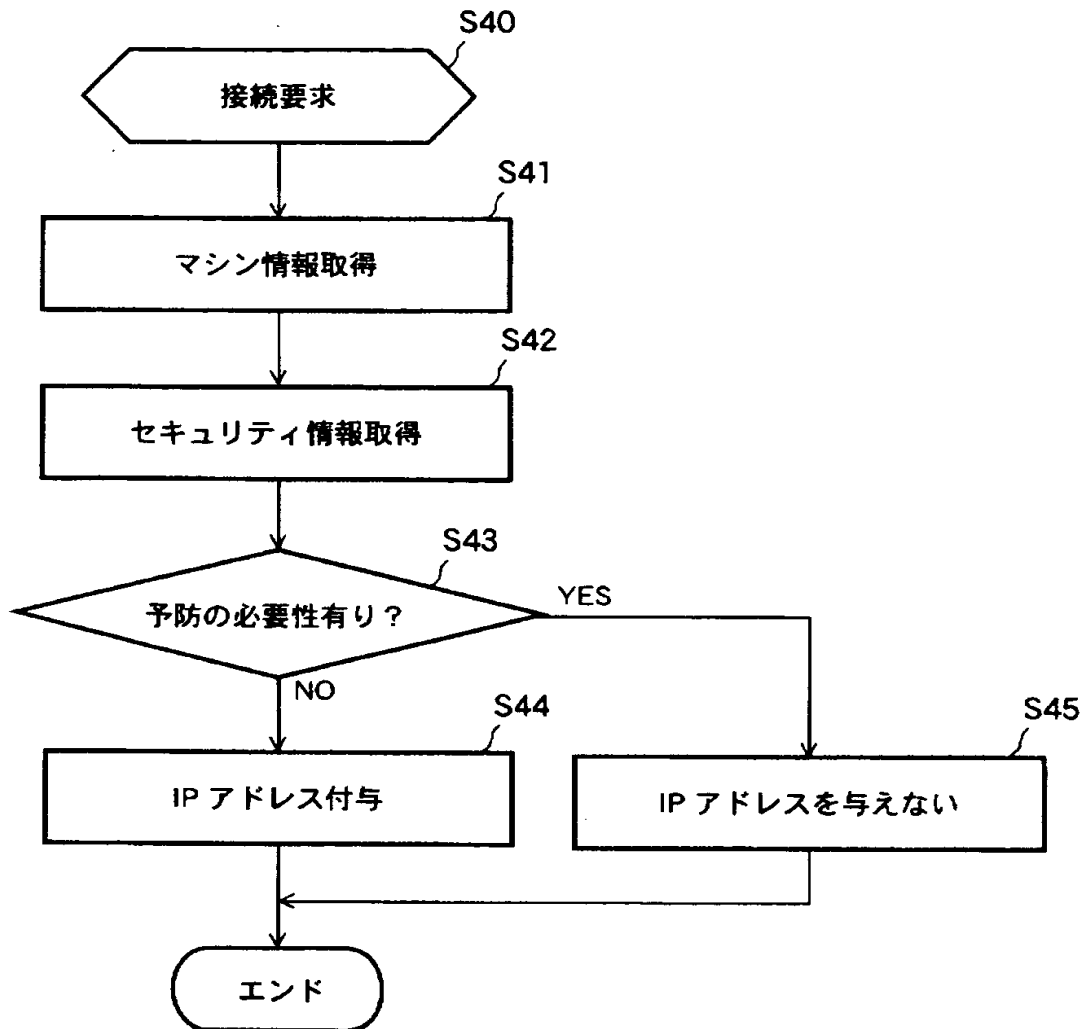
【図12】



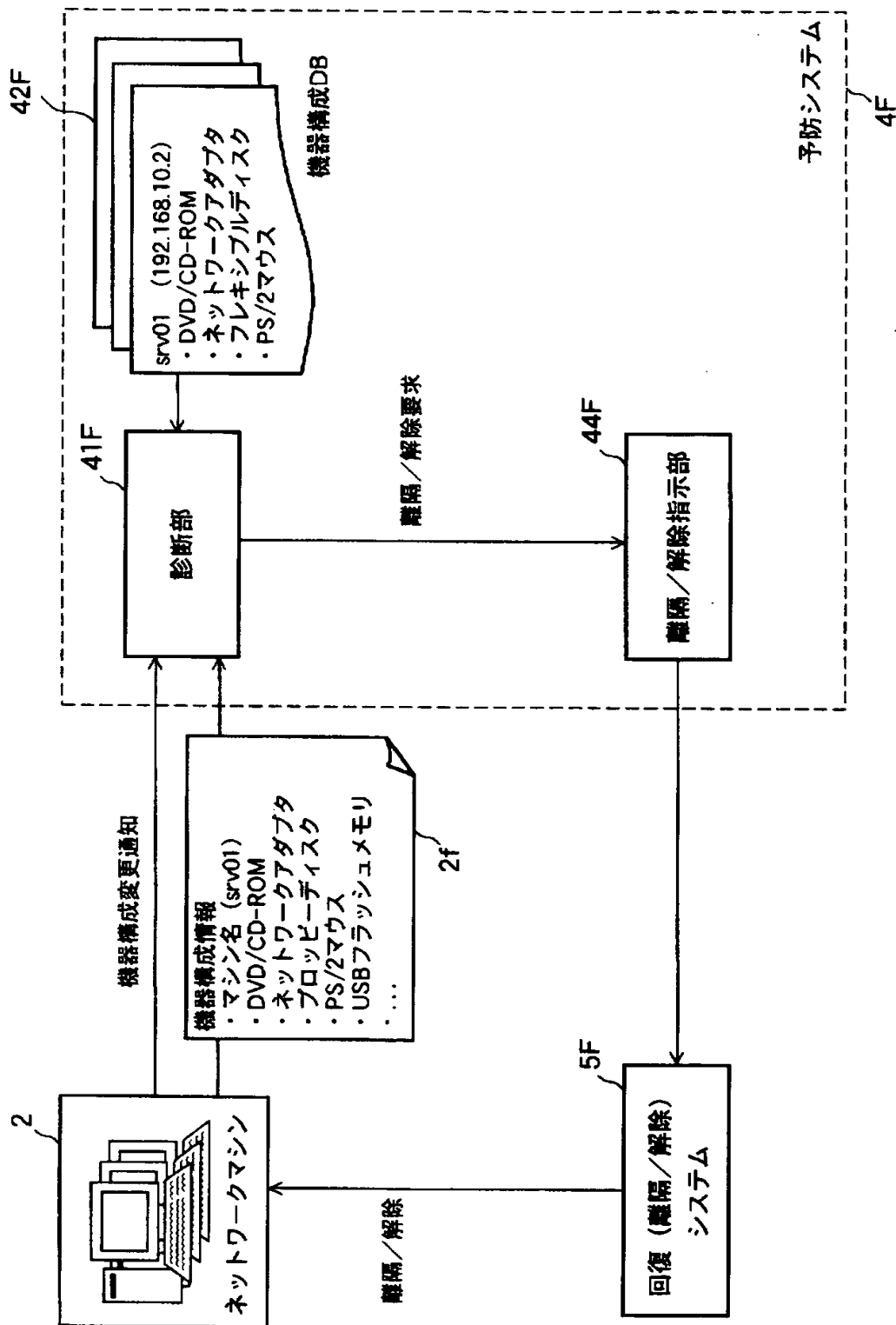
【図13】



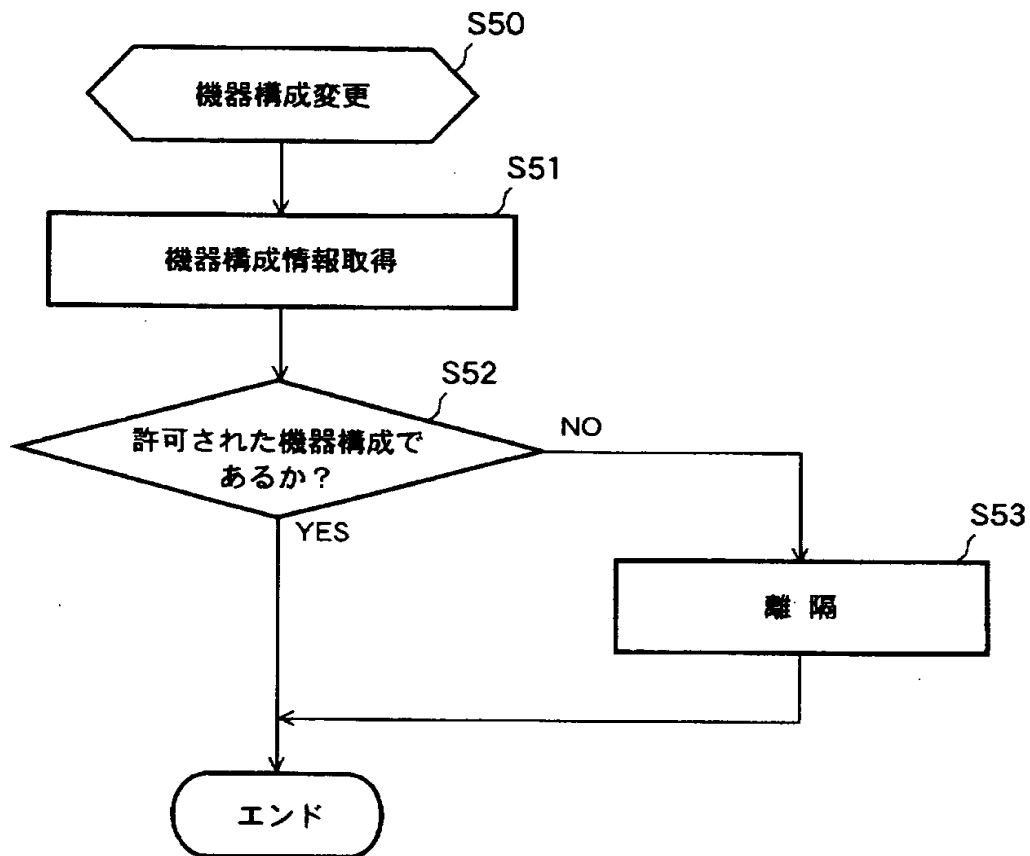
【図 14】



【図 15】



【図 16】

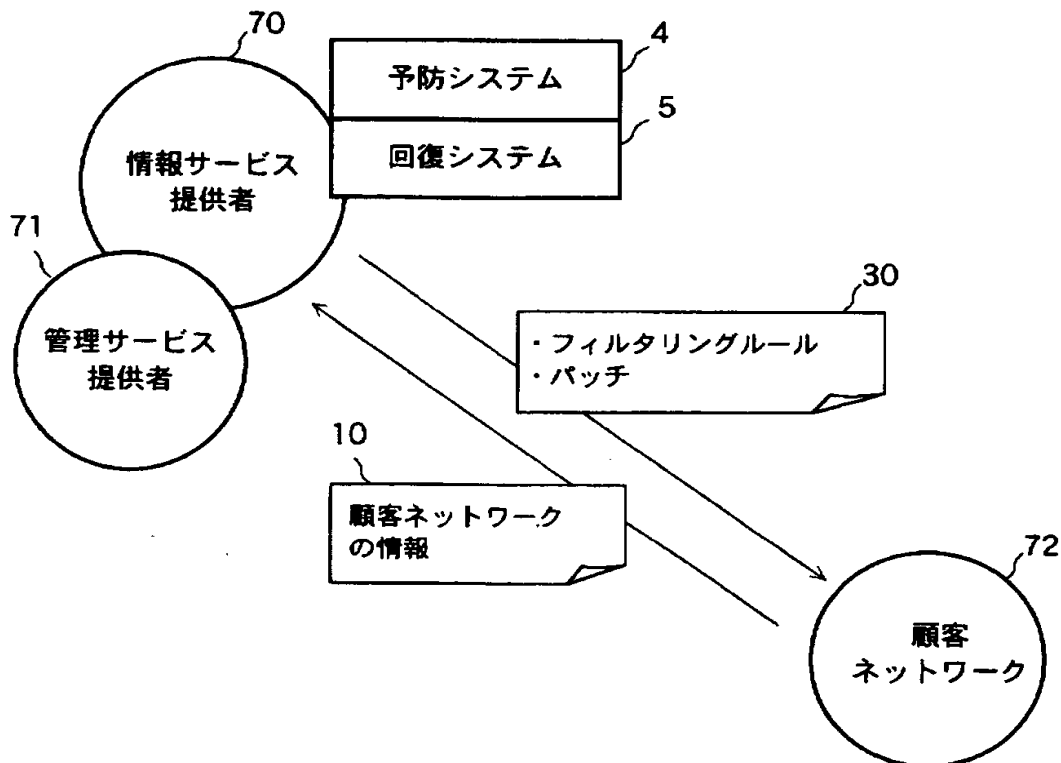


【図 17】

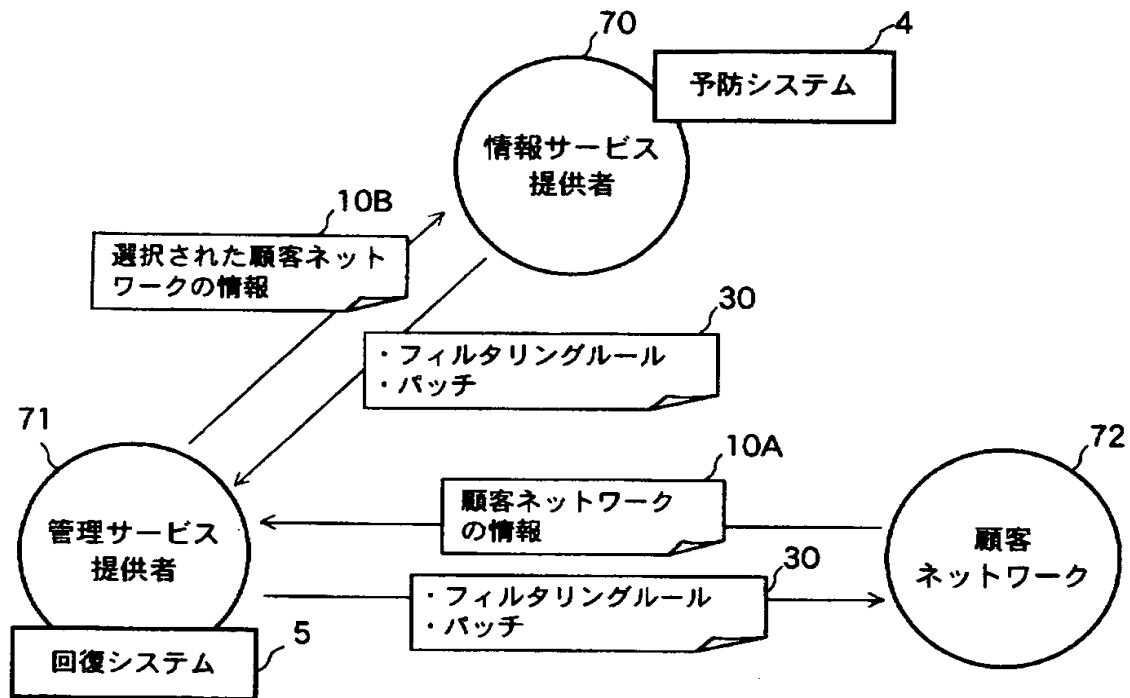
```

[SERVER_NAME]
srv01
[ARCHITECTURE]
sparc
[OS_VERSION]
5.8
[HARDWARE]
SUNW,SPARCstation-20
[INSTALL_PACKAGE]
SUNWadmap
SUNWftpr
SUNWftpu
.
[APPLY_PATCH]
109134-10
109134-27
109618-01
.
[END]
    
```

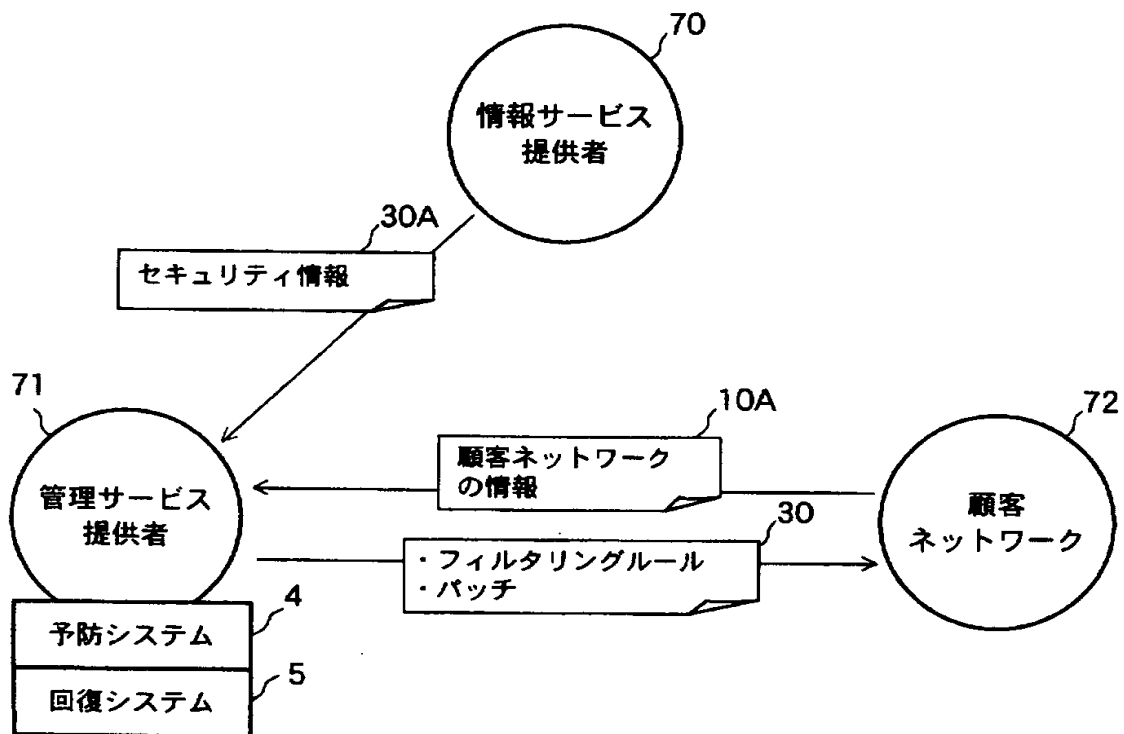
【図 18】



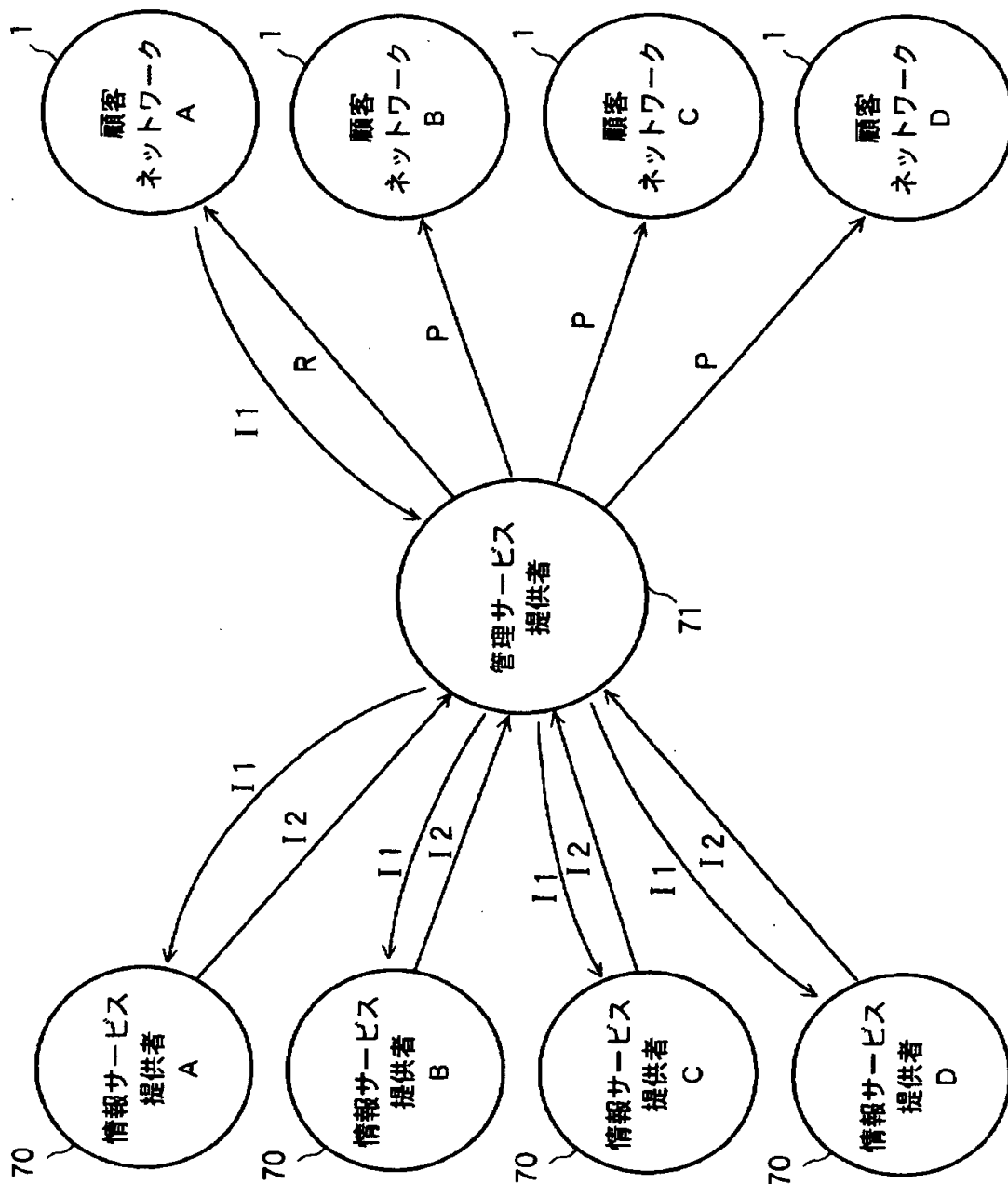
【図 19】



【図 20】



【図 21】



【書類名】 要約書

【要約】

【課題】 ネットワークマシンからマシン情報を取得し、このマシン情報を参照しつつ種々のセキュリティ対策を講じることができ、もって柔軟性に優れ、幅広く適用することが可能なセキュリティ管理装置等を得る。

【解決手段】 ネットワークにおけるセキュリティに関する情報を提供するセキュリティ情報提供装置 3 から取得されるセキュリティ情報と、ネットワーク 1 に接続された少なくとも一つのネットワークマシン 2 から取得されるマシン情報とに基づいて、ネットワークマシンに対して、セキュリティ関連処理の種別とその必要性の有無を判断するセキュリティ診断部 4 1 と、セキュリティ診断部 4 1 による診断結果に基づいて、ネットワークマシンに対して、所定のセキュリティ対策処理を行う予防実行部 4 4 とを備えてなる。

【選択図】 図 2



特願 2 0 0 3 - 0 4 6 2 5 1

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 2 2 3]

1. 変更年月日

1 9 9 6 年 3 月 2 6 日

[変更理由]

住所変更

住 所

神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号

氏 名

富士通株式会社